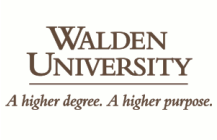

2019

Public Servants' Perceptions of the Cybersecurity Posture of the Local Government in Puerto Rico

Julio C. Rodriguez
Walden University

Walden University

College of Social and Behavioral Sciences

This is to certify that the doctoral dissertation by

Julio Cesar Rodriguez

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Ernesto Escobedo, Committee Chairperson,
Public Policy and Administration Faculty

Dr. Raj Singh, Committee Member,
Public Policy and Administration Faculty

Dr. Timothy Bagwell, University Reviewer,
Public Policy and Administration Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2019

Abstract

Public Servants' Perceptions of the Cybersecurity Posture of the Local Government in Puerto Rico

by

Julio Cesar Rodriguez

MBA, Universidad Metropolitana, 2009

BBA, Universidad del Turabo, 2007

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

February 2019

Abstract

The absence of legislation, the lack of a standard cybersecurity framework, and the failure to adopt a resilient cybersecurity posture can be detrimental to the availability, confidentiality, and integrity of municipal information systems. The purpose of this phenomenological study was to understand the cybersecurity posture of municipalities from the perception of public servants serving in information technology (IT) leadership roles in highly populated municipalities in the San Juan – Carolina – Caguas Metropolitan Statistical Area of Puerto Rico. The study was also used to address key factors influencing the cybersecurity posture of these municipalities. The theoretical framework was open system theory used in combination with a conceptual framework encompassing key dimensions influencing digital government. Data were collected using semistructured interviews with 10 public servants working in IT leadership positions in a municipal setting in Puerto Rico. Data analysis involved horizontalization, reduction, elimination, clustering, thematizing, validation, and development of individual and composite textural descriptions. Participants reported that the cybersecurity posture of their municipalities was resilient. Participants also reported that technological changes, politics, the economy, management support, and processes were key elements to achieve a resilient posture. Findings may be used to empower elected officials, policymakers, public servants, and practitioners to manage and improve elements affecting cybersecurity with the goal of achieving a resilient posture to deliver cybersecurity as a public good.

Public Servants' Perceptions of the Cybersecurity Posture of the Local Government in Puerto Rico

by

Julio Cesar Rodriguez

MBA, Universidad Metropolitana, 2009

BBA, Universidad del Turabo, 2007

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

February 2019

Acknowledgments

I want to thank my father Julio A. Rodriguez for his support during the development of the prospectus. The prospectus was the cornerstone for this research, and his feedback was crucial to achieving clarity and a common understanding. I also want to recognize my friend Patricia Meyertholen who play an essential role during the development of the proposal by providing both moral support and valuable feedback to improve the quality of the manuscript. Dr. Beth Hagens, I am grateful with your support as the methodology expert during the proposal process. I want to give kudos to the public servants who participated in the study. I appreciate everything you do to support government operations and the people; your feedback was invaluable to the outcome of the study. I cannot thank enough the dissertation committee formed by Dr. Ernesto Escobedo and Dr. Raj Singh for all their support during the dissertation process. Dr. Escobedo thank you for pushing me onward and forward. Lastly, I want to thank my family and friend who supported me throughout this journey.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

Information resources have become essential to support the private sector, the government, and the general population. These entities depend on information systems to manage data assets and perform the activities required to fulfill their respective business purposes and mandates. Information systems can be subject to criminal attacks capable of jeopardizing their functionality, as well as related sensitive data. Hackers are the actors responsible for executing these attacks. The term *hacker* was first used to refer to problem solvers and programmers who were responsible for the development of automated systems and computer programs (Taylor, Fritsch, Liederbach, & Holt, 2011). The meaning of hacker has evolved to include cybercriminals such as crackers, script kiddies, black hats, and hacktivists trying to gain or having gained unauthorized access to information systems (Kissel, 2013).

The use of technology as a vehicle to commit crimes has become a common threat (Taylor et al., 2011). The federal government is working to address the challenges and threats affecting cyberspace. Most federal agencies are incorporating cyber divisions to protect and defend their information resources. The Computer Fraud and Abuse Act (CFAA) of 1986 and the Federal Information Security Modernization Act (FISMA) of 2014 are the primary information security policies addressing cyber threats. The CFAA of 1986 regulates illegal hacking against protected computers, including access without authorization or exceeding authorized access. Alternatively, FISMA of 2014 mandates the protection of information technology (IT) infrastructure and services and establishes "a comprehensive framework for ensuring the effectiveness of information security

controls over information resources that support federal operations and assets" (p. 128). Under FISMA of 2014, federal agencies and organizations processing federal information are responsible for implementing security controls in accord with federal "policies, procedures, standards, and guidelines" (p. 128).

Despite regulations such as CFAA of 1986 and FISMA of 2014, the Internet remains a "lawless frontier where bullies, deviants, criminals, and terrorists can roam freely with reckless abandon" (Taylor et al., 2011, p. 2). A comprehensive information security policy may avoid gaps that could be exploited by cybercriminals. Technology is constantly evolving, and these changes can affect the ability of policymakers at all government levels to develop legislation to address the possible impact and consequences of using new technologies. The CFAA of 1986 covers all government computers, as well as nongovernment computers, use for "interstate or foreign commerce or communication" (p. 298). However, FISMA of 2014 is only applicable to entities responsible for federal information and information systems. This situation created a gap in policy for the state and local governments, leaving them without a legal obligation and the absence of a standard framework.

Cyber threats are everybody's concern. State and local governments have started to develop and implement information security policies. For instance, the Oficina de Gerencia y Presupuesto (OGP) de Puerto Rico [Office of Management and Budget (OMB) of Puerto Rico] established Tecnologías de Información Gubernamental (TIG) [Government Information Technology] -003: Security of Information Systems Policy to provide government agencies with guidelines to ensure the confidentiality, integrity, and

availability of the information systems and data assets under their jurisdiction. However, policy-making tends to be reactive to cyber incidents (Bertot, Seifert, & Jaeger, 2015). This situation could result in legislation that is neither up to date nor comprehensive enough to address the complexity of cyber threats. The absence of information security policies and standard frameworks can influence the cybersecurity posture of local governments and affect the safety of their constituents. Furthermore, the cost of implementing cybersecurity measures can be expensive for local governments, especially those in Puerto Rico.

Puerto Rico is an unincorporated territory of the United States that operates as a Commonwealth (Central Intelligence Agency [CIA], 2016). Despite the territory status, Puerto Rico's government branches, administrative divisions, judiciary system, and population size resemble those of a state within the United States. Since 2006, Puerto Rico has been undergoing "a sharper recession than the rest of the United States" (U.S. Department of Treasury, 2015). Puerto Rico's fiscal situation is affecting its ability to pay a public debt of $73 billion (CIA, 2016). This deficit affects Puerto Rico's ability to support government operations, including the protection of information systems and data assets. The purpose of this study was to facilitate understanding of the cybersecurity postures within government municipalities in Puerto Rico and identify the factors influencing these postures. Findings may be used to improve the cybersecurity posture of the local government in Puerto Rico by supporting the security and availability of government systems through the development and implementation of cost-effective measures such as legislation, policies, procedures, and collaboration strategies.

The sections of this chapter introduce the cybersecurity posture of municipalities within Puerto Rico. These sections include the study's background, problem, purpose, and research questions. I also describe the research frameworks that served as the lens to explore the research problem. This chapter also includes the nature of the study, definitions of key terms, assumptions, boundaries, limitations, and significance of the study.

Background of the Study

There is an increasing dependency on information systems, Internet technologies, and cyberspace. The term *technology* encompasses "the development and application of devices for productive processes" (Orrick, 2012, p. 396). These processes are meant to be beneficial to the common good. Unfortunately, criminals are also benefiting from these technologies as a vehicle to commit crimes. Government agencies such as municipalities are taking advantage of technology to facilitate democratic governance, increase citizen participation, perform daily operations, communicate with constituents, and provide public services (Gil-Garcia & Pardo, 2005; Sá, Rocha, & Pérez-Cota, 2015; Saxby, 2015). Municipalities operate the closest to the people and serve as the principal provider of social and public services such as education, health, and infrastructure management. Other government duties include performing as first responders and being accountable for the public safety and emergency management of their jurisdiction (Sylves, 2015). The use of technology to fulfill these mandates is known as e-government and e-democracy.

The Government of Puerto Rico through the enactment of legislation such as the Ley de Gobierno Electrónico de 2004 [Electronic Government Act (E-Government Act)

of 2004] has acknowledged the importance of information resources to promote economic development, improve the timeliness and quality of government services, and foster and preserve public trust. The E-Government Act of 2004 mandated agencies to incorporate IT to conduct government operations and improve their service delivery, performance, and ability to disclose information, thereby facilitating citizen participation. However, concerns about cyberattacks affect people's trust in e-government, especially within small localities (MacManus, Caruson, & McPhee, 2013). Failing to secure the technology behind e-government and e-democracy can have an adverse impact on democracy (Sá et al., 2015; Saxby, 2015). These factors make the cybersecurity posture of local governments a problem worth studying.

Cybersecurity is a complex concept encompassing many challenges and requiring numerous strategies to secure the components encompassing cyberspace. These strategies can include the development, implementation, and management of information security policies, training, education, security controls, and cross-sector partnerships. Cyberattacks can have adverse effects on public safety. For this reason, cybersecurity should be acknowledged as public good within a similar context to public safety (Asllani, White, & Ettkin, 2013). Asllani et al. (2013) pointed out "the role of federal, state, and local governments to implement policies and initiatives that improve the cybersecurity of individuals and organizations" (p. 9). Picazo-Vela, Gutierrez-Martinez, and Luna-Reyes (2012) recognized the need for developing and implementing information security policies to deter data compromise, prevent identity theft, and stimulate compliance with existing regulations. Bertot et al. (2015) agreed on the necessity to address cybersecurity

threats through policy and technical solutions. However, current policy efforts are reactionary and have been unable to catch up to emerging threats and technologies (Bertot et al., 2015).

Public servants at all government levels are responsible for complying with current policies and implementing adequate security controls. However, most federal policies have failed to account for the local government and its domain within cyberspace. This situation could affect the cybersecurity posture of government municipalities and local operating agencies by leaving them more vulnerable to cyber threats. In response, the government must be active in addressing policy gaps and defining adequate security controls to cover the entire echelon of government operations.

Compliance with federal policies like FISMA of 2014 could help develop a resilient national cybersecurity posture and protect the local government's operations, technology investment, mission critical data assets, and other sensitive information. However, FISMA of 2014 is only applicable to federal agencies and organizations processing federal information. State and local government voluntary compliance with federal policy could have a significant impact on the fiscal operations. For instance, voluntary compliance with information security policy such as FISMA of 2014 involves expenditures related to addressing system vulnerabilities, developing security safeguards, implementing security controls, and assessing the cybersecurity posture of the systems. These requirements can increase operational cost and affect the budget of municipal agencies.

According to the U.S. Department of Treasury (2015), “Puerto Rico is deploying onerous and unsustainable emergency liquidity actions” (p. 3) to continue providing government services. The fiscal crisis in Puerto Rico has caused the government to expedite strategies to reduce operational costs. In a continuous attempt to decrease government spending, the governor of Puerto Rico during 2012 to 2016 issued an Orden Ejecutiva (OE) [Executive Order] to repeal the Executive Order OE-2009-009 (2009) that established the office and responsibilities of chief information officer (CIO) of Puerto Rico. Executive Order No. 2015-019 (2015) dismantled the office of the CIO and transferred some of the responsibilities into the Departamento de Desarrollo Económico y Comercio [Department of Economic Development and Commerce] (p. 1). These actions left Puerto Rico without an IT executive and technical advisor responsible for the development and implementation of information security policies, strategic plans, standards, and enterprise architecture.

In the absence of adequate information security policy, local government personnel, including elected officials, public servants, and IT leaders should have a sense of duty to look at other information assurance (IA) strategies that may help to protect their information systems and data assets. However, there is a “significant knowledge gap” (Caruson, MacManus, & McPhee, 2012, p. 11) between IT professionals and public administrators. This gap acts as a policy obstacle affecting the planning and implementation of security controls. According to Caruson et al. (2012), this situation is one of the reasons why the solution to the existing cybersecurity problem may require actors external to the government to take action.

A cybersecurity triad based on collaboration among government levels, the private sector, and the general population can help mitigate cyber threats. Asllani et al. (2013) concluded that "cybersecurity requires…federal, state, and local government organizations; and private organizations and individuals to implement good cybersecurity controls" (p. 13). A compromise in a municipal system could jeopardize the confidentiality, integrity, and availability of interconnected systems, including systems at state and federal levels. Cyber awareness, training, and education are critical factors affecting cyber preparedness. These factors are also crucial for reducing the existing knowledge gap about cybersecurity (Caruson et al., 2012). Given these factors, the federal government established the National Initiative for Cybersecurity Education (NICE) to be responsible "for cybersecurity awareness, education, training, and workforce development" (Paulsen, McDuffie, Newhouse, & Toth, 2012, p. 76).

A resilient cybersecurity posture requires the government, the private sector, and the people to be cognizant of cyber threats, as well as their risks and mitigation strategies. Asllani et al. (2013) placed the government at the top of the cybersecurity triad. This position makes public servants, especially those in IT leadership roles, the first line of defense and increases their need for awareness and education. However, a recent study revealed a significant knowledge gap among IT professionals and public servants, especially in the local government (Caruson et al., 2012). Bertot et al. (2015) stressed the need for education covering cybersecurity risks. Lack of training and awareness can become bureaucratic roadblocks affecting the implementation of security control (Caruson et al., 2012). Allowing public servants to attend cybersecurity-related

conferences and training with the private sector is essential to reduce the existing knowledge gap and foster public-private collaboration.

The private sector also plays a critical role in the nation's critical infrastructure, economy, education, and health. Asllani et al. (2013) explained the importance of public-private partnerships (PPPs) such as InfraGard and the Information Sharing and Analysis Centers. These partnerships facilitate sharing information and devising strategies to protect the nation's critical infrastructure from cyber threats. PPPs are crucial to support the role of the general population within the cybersecurity triad. NICE started working on cyber awareness and education efforts by partnering with "community centers, school districts, and colleges and universities around the United States to help run cyber citizen forums" (Paulsen et al., 2012, p. 78).

Minimal research has been conducted on the local government cybersecurity posture, especially as it relates to Puerto Rico. Existing studies on cybersecurity have focused on the private sector and the federal government. This situation has resulted in a significant gap in knowledge and literature about what local government agencies are doing to protect themselves against cyber threats and preventing or reacting against cyberattacks. Cyberspace represents a relatively new domain that policies have not been able to address with success. It is critical that public servants understand the factors influencing the cybersecurity posture of their organizations.

Studying the cybersecurity posture of municipalities and the factors affecting such postures was necessary to expand the current cybersecurity knowledge base. Exploring the posture of municipalities within Puerto Rico may improve understanding of their

stance and identify influential factors to support the development and implementation of cost-effective strategies to improve cybersecurity at the local government level. These strategies include adopting adequate security standards and guidelines, improving policies and procedures, aligning procurement and acquisition with cybersecurity needs, developing new cybersecurity and privacy training or taking advantage of other government agency's training resources, and implementing partnerships with other government agencies and the private sector. These strategies may be used to facilitate the development of a resilient cybersecurity posture in municipalities within Puerto Rico, as well as other local governments within the United States.

Problem Statement

The absence of legislation, the lack of a standard cybersecurity framework, and the failure to adopt a resilient cybersecurity posture are detrimental to the availability, confidentiality, and integrity of information systems. Municipal governments are benefiting from information systems to perform and manage daily operations. Advances in technology have also enabled criminals to develop new strategies, expand their operations, and increase their ability to reach out to more potential victims, including the government (Taylor et al., 2011). Municipalities are responsible for providing direct social and public services to their constituency. Furthermore, municipalities serve as primary responders and are responsible for the public safety and disaster recovery of their jurisdictions (Sylves, 2015). Cyberattacks against municipalities could be devastating to their governance, the economy, and the well-being of their constituents.

Federal, state, and local governments need to manage similar controlled unclassified information (CUI) to fulfill their mandates. CUI includes personally identifiable information (PII) of constituents and employees, law enforcement operations, and information about critical infrastructures, among other sensitive data (U.S. National Archives and Records Administration, 2018). A compromise on any of these data asset can affect the government's reputation, force unnecessary expenditure, undermine response to emergency events, and disable governance capabilities (Caruson et al., 2012). At the federal level, FISMA of 2014 provides a framework of security controls to protect information resources from cyber threats. However, state and local governments are not subject to federal information security policies such as FISMA of 2014. In the same way as FISMA of 2014, other federal mandates like circulars from the OMB and several Homeland Security Presidential Directives (HSPDs) do not require compliance by these entities.

Caruson et al. (2012) affirmed that there has been minimal research on the cybersecurity posture of local governments and the ability of public servants to manage and implement security controls to mitigate cyber threats. Recent studies on cybersecurity have concentrated on the federal government, leaving a gap in knowledge about this phenomenon at the local level. The cost to voluntarily comply with federal information security policy can affect the operational cost of local governments. Understanding the cybersecurity posture of municipal governments may assist in developing cost-effective strategies to improve the resiliency of the cybersecurity posture of these organizations.

Purpose of the Study

The purpose of this study was to understand the cybersecurity posture of municipalities from the perception of public servants serving in IT leadership roles in Puerto Rico. The study also addressed the primary factors influencing the cybersecurity posture of municipal governments in Puerto Rico. A phenomenological approach was used to address the knowledge gap about the problem. This qualitative study focused on the lived experiences of IT leaders as information-rich cases. In this study, cybersecurity posture was defined as the security status of the municipal "networks, information, and systems based on IA resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes" (Kissel, 2013, p. 179).

Research Questions

Two qualitative research questions (RQs) guided the study. These questions were designed to address the lived experiences of IT leaders regarding the phenomenon under study. The research questions for this study were the following:

RQ1: How do public servants in IT leadership roles perceive the cybersecurity posture of government municipalities in Puerto Rico?

RQ2: What factors do public servants in IT leadership roles perceive as most influential to achieve a resilient cybersecurity posture in government municipalities in Puerto Rico?

Theoretical Foundation

The theoretical framework for the study was the open system theory (OST). This theory originated from the general system theory (GST). Bertalanffy (as cited in Sher, 2004) argued that "studying the smallest elements of phenomena was disadvantageous because that way one lost sight of the whole" (p. 613). Therefore, Bertalanffy (as cited in Sher, 2004) proposed a multidisciplinary approach incorporating theories and concepts from different disciplines to study phenomena as a whole. According to Sher (2004), Bertalanffy's GST emphasizes the arrangements, functions, and relationships of the elements of a system or phenomena. GST has been applied to system engineering, cybernetics, information systems, and social sciences (Bailey, 2005).

The concept of cybersecurity involves most of these areas of study, especially information systems and social sciences. Shafritz, Ott, and Jang (2015) explained that these elements are interconnected and may include "inputs, processes, outputs, and feedback loops, and the environment" (p. 340). OST was relevant to this study because the cybersecurity posture of local government municipalities can be divided into empirical units. These entities include personnel, processes, and technologies. As proposed in OST, changes in one element have positive or adverse effects on other system components affecting the level of resiliency of the cybersecurity posture. Studying cybersecurity as an open system was intended to identify which elements are influencing the security posture of municipalities in Puerto Rico and to explain their relationships.

Conceptual Framework

Cybersecurity consists of multiple realities, particularly when studied from the perspectives of individuals. The conceptual framework was based on the Picazo-Vela et al.'s (2012) key dimensions influencing digital government. This framework consists of six dimensions, including "(1) general context, (2) institutional framework, (3) interorganizational collaboration and networks, (4) organizational structures and processes, (5) information and data, and (6) technology" (Picazo-Vela et al., 2012, p. 506). Figure 1 provides a visual representation of the dimensions influencing digital government.

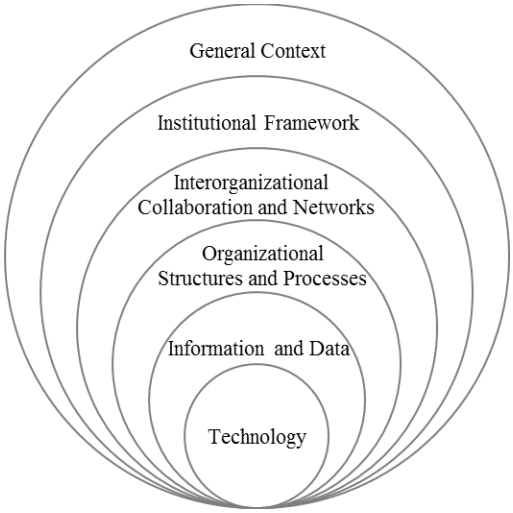

Figure 1. Dimensions influencing digital government. Adapted from "Understanding Risks, Benefits, and Strategic Alternatives of Social Media Applications in the Public Sector," by S. Picazo-Vela, I. Gutierrez-Martinez, and L. F. Luna-Reyes, 2012, *Government Information Quarterly 29*(4), p. 507.

The dimensions in the Picazo-Vela et al.'s (2012) framework were used to capture the complexity of the cybersecurity phenomenon. These interrelated dimensions contributed to the structure of the literature review, the development of interview

questions, the organization of the collected data, and the data analysis and interpretation. The dimensions also provided the lens to identify which elements are influencing the posture of government municipalities in Puerto Rico.

Nature of the Study

The nature of this study was qualitative. I used a transcendental phenomenological design to study the cybersecurity posture of municipalities as a social problem. Most security artifacts are protected from public release by privacy laws like the Freedom of Information Act (FOIA) by Exception 2 (b). However, individuals such as IT leaders provided trustworthy and dependable alternative data sources that were used to study the cybersecurity posture of municipal governments.

Phenomenology focuses on the experience of the participants. The current gap in knowledge and the limitations of privacy regulations made phenomenology a suitable approach to study cybersecurity. These conditions supported the rationale for using a phenomenological approach for performing the collection and analysis of data grounded in participants' experiences. The phenomenon investigated was the perception of public servants in IT leadership roles regarding the cybersecurity posture of municipalities within Puerto Rico and the factors influencing this posture. The perceptions of participants originated from their lived experiences with different cybersecurity concepts.

The key inquiries of the study were related to the ability of municipalities to protect the information resources under their jurisdiction from cyber threats and cyberattacks. The methodology included face-to-face interviews with individuals as the unit of analysis. The sample consisted of public servants working as IT leaders who had

experienced the phenomenon. A strategy incorporating purposeful and criterion sampling was used to identify 10 participants who served as information-rich cases. The semistructured interview protocol included 13 open-ended questions.

The data obtained from the interviews were captured through a combination of field notes, mind maps, and audio recording. Data were organized using NVivo qualitative data analysis software. This software supported the coding, analysis, interpretation, and representation of the data. The data were analyzed through a combination of predetermined and emerging codes. Predetermined codes originated from the conceptual framework. Emerging codes were discovered as part of the data analysis. This methodology was used to describe the cybersecurity posture of municipalities and identify the factors that had the most significant influence on the phenomenon.

Definitions

Scholars agree on the need for concise definitions of the concepts related to the cybersecurity (Craigen, Diakun-Thibault, & Purse, 2014; Kenney, 2015; Tehrani, Manap, & Taji, 2013). Scholars, industries, organizations, and countries adhere to distinct definitions of cybersecurity concepts. Craigen et al. (2014) argued that not having a consistent meaning for these concepts could affect the development of solutions capable of addressing the complexity of cybersecurity. To provide uniform, concise, and reliable definitions, the *Glossary of Key Information Security Terms* was the primary source for defining the concepts related to the study. This glossary was developed by the National Institute of Standards and Technology (NIST) in alignment with the Committee for National Security Systems.

Agency: Government entities of the executive branch of the government, public corporations, municipalities and legislatures, special corporations for municipal development, municipal corporations, boards and those entities under the jurisdiction of this branch (Ethics in Government Act, 2011).

Attacker/hacker: An unauthorized user who attempts to or gains access to an information system (Kissel, 2013).

Availability: The property of being accessible and usable upon demand by an authorized entity (Kissel, 2013).

Compromise: Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred (Kissel, 2013).

Confidentiality: The property that sensitive information is not disclosed to unauthorized individuals, entities, or processes (Kissel, 2013).

Controlled unclassified information (CUI): Unclassified information (a) pertinent to the national interests of the United States or the important interests of entities outside the federal government, and (b) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits (Kissel, 2013).

Critical infrastructure: System and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters (Kissel, 2013).

Cyber incident: Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and the information residing therein (Kissel, 2013).

Cyberattack: Attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure, or destroying the integrity of the data or stealing controlled information (Kissel, 2013).

Cybersecurity: The ability to protect or defend the use of cyberspace from cyberattacks (Kissel, 2013).

Cyberspace: A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (Kissel, 2013).

Data asset: A system or application output file, database, document, Web page, and service that may be provided to access data from an application (Kissel, 2013).

Information assurance (IA): Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities (Kissel, 2013).

Information resources: Information and related resources, such as personnel, equipment, funds, and IT (Kissel, 2013).

Information security policy: Aggregate of directives, regulations, rules, and practices that prescribe how an organization manages, protects, and distributes information (Kissel, 2013).

Information sharing: Requirements for information sharing by an IT system with one or more other IT systems or applications, for information sharing to support multiple internal or external organizations, missions, or public programs (Kissel, 2013).

Information system: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (Kissel, 2013).

Information technology (IT): Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information (Kissel, 2013).

Integrity: The property that sensitive data have not been modified or deleted in an unauthorized and undetected manner (Kissel, 2013).

IT leaders: Individuals responsible for the IA of a program, organization, system, or enclave (Kissel, 2013).

Personally identifiable information (PII): Any information about an individual maintained by an agency, including (a) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (b) any other information that is

linked or linkable to an individual, such as medical, educational, financial, and employment information (Kissel, 2013).

Public servant: Person in the government involved in the formulation and implementation of public policy or not, but performs as permanent or temporary, with or without pay. It also includes the contractor whose contract is equivalent to a position or responsibilities related to public policy (Ethics in Government Act, 2011).

Resilience: The ability to quickly adapt and recover from any known or unknown changes to the environment through the holistic implementation of risk management, contingency, and continuity planning (Kissel, 2013).

Security controls: The management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information (Kissel, 2013).

Security posture: Status of an enterprise's networks, information, and systems based on IA resources and capabilities in place to manage the defense of the enterprise and to react as the situation changes (Kissel, 2013).

Security program plan: A formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management security controls and common security controls in place or planned for meeting those requirements *(*Kissel, 2013).

Sensitive information: Information, the loss, misuse, or unauthorized access to or modification of, that could adversely affect the national interest or the conduct of federal

programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (Kissel, 2013).

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, or denial of service (Kissel, 2013).

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source (Kissel, 2013).

Assumptions

Several assumptions were critical to the methodology, particularly the sampling strategy. The assumptions were related to the trustworthiness of the data, the selection of research sites, and the population sample. The unit of analysis consisted of IT leaders as individual entities. Privacy regulations protected against the disclosure or public release of cybersecurity documents. I assumed that the IT leaders would provide trustworthy and dependable data. Information security policies prevent organizations from sharing cybersecurity-related information.

The sites for the study included municipalities within the San Juan – Carolina – Caguas Metropolitan Statistical Area (MSA) as defined by the OMB Bulletin 13-01. The plan to target these municipalities emerged from the assumption that highly populated municipalities manage larger budgets, provide additional services, and require more

complex information resources than less populated municipalities. Highly populated municipalities need additional resources to support and sustain the continuity of their government operations for a larger population. This assumption justified considering municipalities within the San Juan – Carolina – Caguas MSA for the study.

The conditions within highly populated municipalities had an influence on the selection of IT leaders for the study. Government agencies with additional functions, resources, and complex information systems enhanced the lived experiences of IT leaders working within these environments. The exposure of the participants to these conditions supported their inclusion as information-rich cases for the study. This assumption supported the use of purposeful and criterion sampling to identify participants that could serve as information-rich cases. Finally, I assumed that participants would be available to participate in interviews and provide member checking.

Scope and Delimitations

The purpose of the study was to explore the cybersecurity posture of municipalities within the San Juan – Carolina – Caguas MSA. This posture was related to the local government position to protect and defend information systems and data assets through the management of information resources and security policies. The purpose also included the analysis of the factors that may be influencing the administration of information resources and security controls. This focus was chosen to address the knowledge gap about the phenomenon, to develop strategies to support the local government's cybersecurity resilience, and to identify areas for future research.

Delimitation consists of determining the limits or boundaries for the research (New Oxford American Dictionary, n.d.). Patton (2002) described delimitation as a process to eliminate "irrelevant, repetitive, or overlapping data" (Phenomenological Analysis, para. 6) to focus on the data that are more relevant for the study. The study was delimited to the population of public servants acting in IT leadership roles within the San Juan – Carolina – Caguas MSA. The Government of Puerto Rico defines public servant as any person working within the government, including permanent, temporary, contracted, and without pay employee (Ethics in Government Act, 2011). This delimitation excluded participants from less populated municipalities that did not provide the conditions to support the development of IT leaders as information-rich cases.

The theoretical foundation for the study was limited to the OST and the dimensions influencing digital government (Picazo-Vela et al., 2012). Other related frameworks were excluded for not been relevant to the nature of the problem. For example, the complex adaptive systems framework addresses the behaviors of known agents within a system. These behaviors include "emergence, stability or chaos, adaptation, and attraction" (Morrell, 2005, p. 72). On the other hand, OST was designed to identify system components and examine their relationship.

The outcomes of this study may contribute to the improvement of cybersecurity resilience of government and nongovernmental organizations in and outside of Puerto Rico. However, the scope and delimitations of the study did not provide for a direct transferability of the results. Puerto Rico's governmental structure resembles that of a U.S. state. Puerto Rico is a commonwealth with an executive, legislative, and judiciary

branch. Similar to U.S. states, Puerto Rico's administrative division includes a state government with an elected governor and jurisdictions or districts known as municipalities, each with an elected mayor. Also, the legal system in Puerto Rico consists of civil law within the context of the federal system (CIA, 2016). According to the U.S. Census Bureau (2015b), Puerto Rico ranks 30 in population size among the 50 states and territories with a total of 3,474,182 people. This similarity supported the transferability of the research methodology and design to study other local governments within the United States.

Limitations

The dependability of the data was crucial to the quality and significance of the study. The primary data source consisted of interviews with public servants in IT leadership roles to obtain their perceptions of the cybersecurity posture of the municipalities, as well as the factors influencing the perceived posture. Participants who lacked such experiences with cybersecurity at the local government could have affected the dependability of the data. Criterion sampling takes into consideration cases meeting a "predetermined criterion of importance" (Patton, 2002, Criterion sampling, para. 1). The criteria included at least 2 years of experience with the phenomenon as a senior IT professional. These conditions were essential to support the relevance of the data.

The availability of the participants limited the scope of the study. The interviews were planned to take place in 2017. In some municipalities, this was the first year of the new administration after the 2016 election. These municipalities could have been waiting to appoint their IT leadership, or the appointed executives may have been working on

projects that may have affected their availability to participate. Reasonable measures to address this limitation included the identification of additional municipalities and participants within the San Juan – Carolina – Caguas MSA as candidates for the study. However, a Category 5 hurricane struck the island, leaving most of the population without electricity and water. The local government was actively engaged in disaster response and recovery. The interviews were performed in May 2018. External threats such as the lack of literature relating to cybersecurity at the local government level also presented a limitation. However, literature about the federal and state levels was examined in the literature review.

Significance of the Study

Significance to Practice

Understanding the cybersecurity posture of municipalities supported advances in practice and policy. The results helped to provide knowledge, identify skills, and promote attitudes to benefit IT leaders and policymakers on achieving a resilient cybersecurity posture. The study addressed the factors influencing such postures. Identifying and understanding these factors was crucial to provide comprehensive research-based solutions to improve the administration of information security programs and policies.

Significance to Theory

Studying the cybersecurity posture of municipalities resulted in a significant contribution to the discipline of public policy and administration. Cyberattacks can jeopardize government operations, the economy, and the well-being of constituents. These risks can cause social and economic injustice to individuals and communities

within the affected jurisdiction. The knowledge gap about this phenomenon represented a challenge to scholars in the discipline. Contributing to the body of knowledge provided better understanding and served as the foundation for future investigations targeting areas of relevance to cybersecurity at the municipal level.

Significance to Social Change

The outcomes of this study contributed to positive social change by empowering elected officials, public servants, IT leaders, and community members with knowledge about why it is essential to secure information systems and how to identify resources and policies to support cybersecurity. Also, public servants and IT leaders could develop skills to reassign resources, implement policies, and establish procedures to protect information systems and data assets from cyberattacks. Further, community members may become aware of cyber threats and assume an active role in supporting the government in the implementation of measures to improve their cybersecurity posture. These results may improve the resiliency of cybersecurity at the local, national, and international government levels.

Summary and Transition

Information resources are used to facilitate day-to-day tasks for the government, the private sector, and the people. Technology has also provided the opportunity to digitalize traditional criminal behavior (Taylor et al., 2011). Criminals have been able to improve their illegal operations, develop new illicit strategies, and expand their target to include the government. According to Caruson et al. (2012), cyberattacks can distress the government’s reputation, expenditure, and governance.

Internet technologies and cyberspace are relatively new areas for which policy has not been able to become accustomed. Also, technology and its uses are constantly evolving, which further impairs policy efforts to address cyber threats. The federal government has enacted information security policies, including legislation, circulars, and directives, to provide a standard security framework and controls to protect information resources. However, most of these policies have been focused on the federal government, and compliance has not been required for state or local governments. This circumstance generated a policy gap that fails to address cybersecurity at the local government level.

This qualitative study addressed the security posture of municipalities within Puerto Rico. Additionally, the study addressed the factors influencing the cybersecurity posture of these organizations. The study targeted highly populated municipalities within the San Juan – Carolina – Caguas MSA to explore a population with more experience with the phenomenon. Reducing the knowledge gap on the cybersecurity posture of municipalities may contribute to the development and implementation of cost-effective strategies and safeguards to mitigate cyber threats. In Chapter 2, I review the literature related to the study.

Chapter 2: Literature Review

The use of technologies such as computers, cloud services, e-mail, and social media facilitates the daily living of individual, private sector, and government entities. Technology has also increased the exposure of these entities to cyber threats. Tehrani et al. (2013) agreed that advances in technology are beneficial to society, but also useful for criminals and terrorist. These actors are taking advantage of technology to commit illicit activities from cyberspace. Furthermore, illicit activities such as cyberattacks can be executed from anywhere in the world against any target, including the government (Tehrani et al., 2013).

The problem addressed in the study was the absence of legislation, the lack of a standard security framework, and the failure to adopt a resilient cybersecurity posture. These conditions can be detrimental to the availability, confidentiality, and integrity of local government systems. Municipalities are taking advantage of information systems to manage their operations and deliver public services. Further, municipal agencies are responsible for providing direct social and public services to their constituents. According to Sylves (2015), local governments are primary responders with responsibilities for the public safety and disaster recovery of their jurisdictions. Cyberattacks against municipal systems can have negative consequences on local governance, public services, public safety, and the economy.

Cybersecurity represents a significant challenge in the preservation of national security, public safety, and the economy (Chen & Dongre, 2014; Roesener, Bottolfson, & Fernandez, 2014). Furthermore, the increasing social dependency on information systems

and new technologies is causing an upsurge of cyber threats and systems vulnerabilities, including severity and the frequency of cyberattacks (Kazemi, Khajouei, & Nasrabadi, 2012). Lozowski (2015) discussed the results of a recent survey, which included 678 participants from the United States. Lozowski explained that about 75% of participants agreed that the severity of cyberattacks has increased. Similarly, 68% agreed that cyberattacks have increased in frequency (Lozowski, 2015). These conditions make adopting a resilient cybersecurity posture imperative for individuals and organizations.

Critical infrastructures such as power grid, mass transit, and financial systems are at risk of sophisticated cyberattacks capable of affecting lives and the economy (Roesener et al., 2014). The U.S. government understood the continuing growth of cyber threats against critical infrastructure and recognized it as one of the most serious security challenges that could affect national and economic security (Executive Order No. 13,636, 2013). In response to the threats to critical infrastructure, the federal government enacted Executive Order 13,636: Improving Critical Infrastructure Cybersecurity (2013) and the Presidential Policy Directive (PPD)-21: Critical Infrastructure Security and Resilience (2013). These policies appoint federal agencies as the responsible parties for identifying and helping secure critical infrastructure (Executive Office of the President, 2013).

State and local governments sometimes in partnership with the private sector are responsible for managing utilities, communication, transit, and financial systems. Cyberattacks against municipal infrastructures can affect hospitals, businesses, and government facilities. Moreover, attacks against transit systems can disturb timely, affordable, and necessary access to health, education, businesses, and government

services (Fok, 2015). Municipalities also depend on financial systems to manage payroll and administer government operations such as taxation and public services for their jurisdiction. Financial systems contain CUI, including PII. Taylor et al. (2011) affirmed that cybercrimes such as "identity theft and Internet fraud are constantly rising" (p. 2). Cyberattacks against municipal systems can affect the availability to meet their mandates and preserve the confidentiality of the data assets that could be used to commit identity theft and fraud.

Executive Order 13,636 (2013) and PPD-21 (2013) identify state and local governments as critical infrastructure owners and define their roles as collaborators. However, federal information security policies are not necessarily applicable to nonfederal entities. Furthermore, these policies provide a set of voluntary security frameworks and controls. For instance, Executive Order 13,636 (2013) requires the establishment of a voluntary program supporting "the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities" (Sec. 8). However, the voluntary adoption of these security frameworks and controls represent an additional level of effort that could impact operating costs. Governments without the appropriate budgetary resources or those undergoing fiscal crisis such as Puerto Rico may not be able to adopt these requirements.

The next sections of this chapter include the literature search strategy, theoretical and conceptual foundations, and the literature review. The literature search strategy includes the list of databases, search engines, terms, and conditions used to identify relevant literature. The theoretical and conceptual frameworks cover the previous

application, rationale, and relation to the OST and the dimensions influencing digital government to the study of the cybersecurity posture of local governments in Puerto Rico. The chapter also includes a review of the current literature related to the concepts and elements of cybersecurity. The chapter concludes with a summary of key themes and findings from the literature review.

Literature Search Strategy

The literature search strategy consisted of a combination of scholarly databases, government websites, search engines, and books. A total of four scholarly databases, including LexisNexis, ProQuest Central, ProQuest Dissertations & Theses @ Walden University, and Science Direct were used in the literature search process. In addition to the scholarly databases, government websites from the U.S. federal government and Puerto Rico were used to search for literature. U.S. federal government websites included U.S. Department of Homeland Security, U.S. Census Bureau, OMB, CIA, and the Executive Office of the President. Government websites for the Commonwealth of Puerto Rico included Departamento de Estado de Puerto Rico [Puerto Rico Department of State], Oficina del Contralor de Puerto Rico [Office of the Comptroller of Puerto Rico], OGP, and Portal Oficial del Estado Libre Asociado de Puerto Rico [Commonwealth of Puerto Rico Official Government Web Portal]. Google was the primary search engine used throughout the literature search process to navigate websites and search for terms.

The terms used in the literature search included *information technology*, *information system*, *cybersecurity*, *cyber security*, *information security*, *local government*, and *United States*. Other terms, including *information assurance* and *Puerto*

Rico, were used in ad hoc searches with no relevant results. Depending on the query capabilities of the database, website, and search engine, these terms were combined using the AND search operator and the OR search operator. The main combination of terms contained cybersecurity, cyber security, and information security.

The iterative search process included ad hoc searches for each term and analysis of the outcomes. Based on the analysis of the results, the search terms were combined, and additional criteria were added. The combination of terms returning the most relevant results was *cybersecurity OR cyber security OR information security AND local government AND United States*. Additional criteria, including limitation to only full text, peer-reviewed, and publication date, were used to ensure accessible, trustworthy, and relevant results. These conditions were applied to searches in ProQuest and Science Direct.

There was limited research about cybersecurity at the state and local government level. All searches returned many articles related to cybersecurity. However, the articles were not directly related to the phenomenon, especially not at the local or municipal level. Independent of the efforts to limit the results to local and municipal governments, the outcomes were relevant to national and international levels. Several strategies were used to compensate for the shortage of literature about the phenomenon at the local government level. First, the search outcomes were limited to literature related to a national level and below with priority for both state and local governments. Further, websites from the U.S. federal government and Puerto Rico were searched for laws,

policies, and guidance related to cybersecurity and related concepts. Also, Lexis Nexis was used to search for laws enacted by the government of Puerto Rico.

Theoretical Foundation

The concept of cybersecurity posture was the phenomenon investigated, especially as it related to government municipalities. NIST explained the concept of security posture as the stance of an organization's information resources "based on IA resources and capabilities in place to manage the defense of the enterprise and to react as the situation changes" (Kissel, 2013, p. 179). This definition made cybersecurity posture a multidimensional concept involving aspects such as people, technology, policies, processes, and organizational elements.

Organizations can be studied and described within the context of an open system (Burke, 2011). Municipalities are organizations that, like open systems, are contingent to the dynamic interaction of internal and external dimensions within their environment. These interactions made OST a suitable theoretical framework for the study. OST emerged from GST. Based on the GST, scholars such as Von Bertalanffy, Katz, and Kahn outlined 10 distinctive characteristics present within open systems (Burke, 2011). These characteristics include the importation of energy, throughput, output, cycles of events, negative entropy, negative feedback, steady-state, differentiation, integration and coordination, and equifinality (Burke, 2011).

The major theoretical proposition was that organizations need an energy source to generate the product and services related to their business purpose and required for their survival. This energy comes from their environment in the form of "money, raw

materials, or the work of people" (Burke, 2011, p. 56). The energy goes through different events as the throughput to produce outputs in the form of product or services. These events are considered cyclical. During these cycles, organizations are subject to entropy that could affect their existence (Burke, 2011).

Feedback from the environment can be used to develop courses of action to support the stability of the organization. After achieving a level of stability, the organization can enter a process of differentiation focused on the growth and specialization of operations (Burke, 2011). This process goes hand and hand with the need to integrate and coordinate among the different organizational and environmental elements. Lastly, the concept of equifinality relates to the flexibility to achieve the same goal from different courses of action (Burke, 2011).

In the case of cybersecurity, municipalities need energy to manage the events supporting the implementation and maintenance of security controls. These controls help to safeguard the municipalities from cyber threats and deliver cybersecurity as a service. The processes and the events related to the security controls are cyclical. Further, municipalities experiencing loss of energy such as budget cuts, personnel reduction, and other events affected by negative entropy that could result in successful cyber incidents. For this reason, the use of information and feedback is critical to developing courses of action capable of improving the cybersecurity posture of the municipalities. A resilient cybersecurity posture could facilitate reaching a steady-state that allows the municipalities to work on differentiation and coordination strategies. Lastly, the principle equifinality gives municipal IT leaders the opportunity to take the appropriate paths to

achieve a more desirable posture.

According to Bailey (2005), the GST has been used to study phenomena related to information systems and social sciences. Further, OST has been used to investigate organizations and information system management (Burke, 2011). Johnson (2012) used systems engineering as an application of the system theory to analyze federal governance practices for protecting critical infrastructure from cyberattacks. According to Johnson, using systems engineering to study cyber terrorism provided the ability to concentrate on different elements related to the environment, the market, and the people. Understanding the different elements related to cyber terrorism can help to develop controls to protect critical infrastructure. Johnson affirmed that the system theory could facilitate the understanding of cyber terrorism as a system and support the process to sustain or improve the posture of critical infrastructure.

Baker (2013) used a conceptual framework based on the GST to study the phenomenon of information sharing among public safety agencies. Baker described these agencies as open systems interacting with each other. As proposed in the GST, changes in one element can affect other interrelated elements and the system as a whole. This principle is also true for public agencies where changes in any aspect of the organization "can affect the entire organizational system" (Baker, 2013, p. 16).

This research concentrated on studying municipalities as organizations and their cybersecurity postures as part of their IT management from a perspective of public policy and public administration which relates to the field of social sciences. Organizations such as municipalities encompassed interconnected elements, including "inputs, processes,

outputs, and feedback loops, and the environment" (Shafritz et al., 2015, p. 340). Also, their cybersecurity posture can be divided into interconnected elements. The OST proposed that changes in one element can affect other interconnected system components. Therefore, changes in one element can have positive or adverse effects on the resiliency level of the cybersecurity posture. These conditions support the rationale for choosing OST as the theoretical foundation for the study.

Gil-Garcia and Pardo (2005) agreed that IT-related phenomena are multidimensional and encompass factors beyond "technological complexity" (p. 188). Gil-Garcia and Pardo recognized that irrespective of the diversity of challenges affecting IT projects, "notable consistencies exist across the disciplines" (p. 188). Gil-Garcia, Pardo, and Baker (2007) emphasized the importance of understanding the organizational and social factors influencing the IT phenomenon. Further, Gil-Garcia et al. recognized systems theory as an approach capable of providing a holistic view of IT phenomenon. Therefore, studying cybersecurity as an open system served as the theoretical lens to identify and explain the relationship of the elements influencing the security posture of government municipalities in Puerto Rico. The OST encompassed characteristics related to the internal and external dimensions of the organization, including their people, interorganizational collaboration, structures, processes, and technology.

Conceptual Framework

Previous IT-related research shared the need for a framework capable of capturing multidimensional elements. According to Jiang and Klein (2000), researchers agreed "that system success is a multidimensional concept" (p. 4). Jiang and Klein were two of

the primary researchers contributing to the conceptual framework that was used during this study. Jiang and Klein employed surveys to study risks affecting IT project performance, especially as it related to software development. A crucial part of the research was to identify common project risks. Jiang and Klein discovered that the absence of expertise and clear roles had a substantial impact on project effectiveness. Gil-Garcia et al. (2007) explained that "recognizing the importance of multiple factors for a more comprehensive view of the phenomenon is not unique to systems development and extends to information systems research in general" (p. 4).

Based on the multidimensional aspect of IT and organizational phenomena, Picazo-Vela et al. (2012) developed a framework that was used as the scholarly framework for this research. For this study, the framework was referenced as the dimensions influencing digital government. The framework consists of six dimensions starting with a general context covering the environmental features surrounding the phenomenon. In the case of cybersecurity posture, this element included "economic, political, and social" (p. 507) characteristics affecting the municipal cybersecurity posture. On the other hand, the institutional framework consisted of policies such as "laws, regulations, norms or any other rule" influencing the cybersecurity posture of government municipalities. Picazo-Vela et al. (2012) described this dimension as complex and crucial as it defines the legal environment influencing governmental action.

The interorganizational collaboration dimension encompasses the development and sustainment of partnerships with parties who could contribute to advances related to the phenomenon. According to Picazo-Vela et al. (2012), the use of professional

networks, including nonprofit and private organizations can facilitate problem-solving and achieve better solutions. The level of collaboration and networking with other organizations could have a significant impact on the cybersecurity posture of municipalities. On the contrary, organizational structures and processes consist of the internal structure, procedures, and strategic planning of a given organization. Picazo-Vela et al. stated that these elements could directly affect the performance of the organization. For instance, the centralization or decentralization of cybersecurity-related tasks could influence the posture of the organization. Similarly, technical, operational, and administrative procedures could have a positive impact on the municipal posture.

Information is another essential dimension of the conceptual framework. Picazo-Vela et al. (2012) stressed that "lack of high-quality data or information may cause project delays or even failure" (p. 507). In cybersecurity, not having information on how to safeguard information resources and data assets could result in a cyber incident or compromise. The last dimension encompassed "hardware, software, and infrastructure technologies" (Picazo-Vela et al., 2012, p. 507). Access to the appropriate technology and the ability to implement it properly are crucial to supporting a resilient cybersecurity posture. Also, the use of incompatible and untested technologies is a potential source of problems and security challenges (Picazo-Vela et al., 2012).

Related conceptual frameworks have been applied in previous studies to investigate phenomena like cybersecurity. Jiang and Klein (2000) formulated a summary of project management risks based on contemporary literature to examine the effect of the risks on the distinct phases of system development. Understanding these risks and

their impacts can contribute to the development and adoption of controls to mitigate risks and improve IT project performance. Gil-Garcia and Pardo (2005) used this study as the foundation for the development of a conceptual framework to capture the factors affecting government IT initiatives. The research was aimed at the federal government but recognized the importance of developing strategies to advance IT initiatives at the state and local government level. Gil-Garcia and Pardo (2005) categorized key factors affecting government IT initiatives into five groups, including "(1) information and data, (2) information technology, (3) organizational and managerial, (4) legal and regulatory, and (5) institutional and environmental" (p. 190).

A few years later, Gil-Garcia et al. (2007) used this framework to investigate "the use of comprehensive prototyping" (p. 2) as a method for understanding emerging technologies. The factors affecting government IT initiatives provided the framework to support the understanding of organizational and social elements affecting systems development. Picazo-Vela et al. (2012) developed a 6-layer framework based on the Gil-Garcia and Pardo's framework to identify the risks and benefits of social media as a government IT initiative. Picazo-Vela et al. (2012) developed a more comprehensive framework that consolidated legal and regulatory factors within an institutional framework, separated environmental factors into a different dimension, and added a layer to account for technology. Figure 2 shows a side by side comparison of the frameworks.

The concepts applied by Jiang and Klein (2000), Gil-Garcia et al. (2007), and Picazo-Vela et al. (2012) proved beneficial for studying phenomena related to IT management from a multidimensional perspective. Furthermore, Gil-Garcia et al. (2007)

and Picazo-Vela et al. (2012) used these concepts to gain an understanding of the factors affecting the management of IT initiatives and new technologies within the government. Cybersecurity is a critical multidimensional discipline within IT. The modification made by Picazo-Vela et al. (2012) gave the framework the complexity to capture the essence of the cybersecurity phenomenon, especially as it relates to the local government. The dimensions influencing digital government framework was beneficial to the formulation of interview questions, as well as to the collection, organization, analysis, and interpretation of research data, and literature.

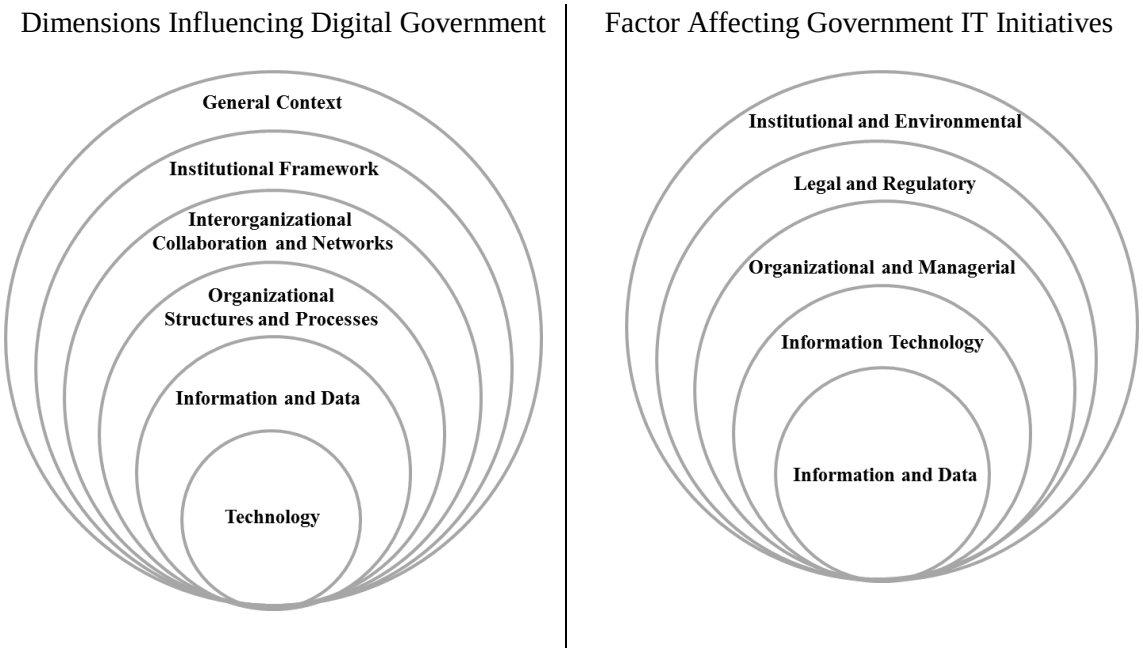

Figure 2. Comparison of conceptual frameworks influencing digital government. Adapted from "Understanding Context through a Comprehensive Prototyping," by J. R. Gil-Garcia, T. Pardo, & A. Baker, 2007, Proceedings from HICSS '07: Experience: A Testbed Research Strategy for Emerging Technologies.

Literature Review

NIST defines cybersecurity as "the ability to protect or defend the use of cyberspace from cyberattacks" (Kissel, 2013, p. 58). Like NIST, there are many other

definitions of cybersecurity. Unfortunately, the absence of a uniform definition can be an obstacle for interdisciplinary advances and solutions for addressing the complexity of cybersecurity. For these reasons, Craigen et al. (2014) took into consideration some of the most commonly accepted definitions of cybersecurity to develop a comprehensive interpretation. Craigen et al. (2014) defined the concept of cybersecurity as "organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights" (Craigen et al., 2014, p. 17). The elements in the dimensions influencing digital government are aligned with this definition of cybersecurity. For this reason, the dimensions of the framework were used to structure the literature review. Most of the articles reviewed utilized qualitative methodology, literature review, and secondary data.

General Context Influence on Cybersecurity

According to Picazo-Vela et al. (2012), general context incorporates economic, political and social environmental factors. Achieving a common understanding of cybersecurity-related concepts is an important component of the general context dimension. Kenney (2014) performed a literature review to explore the differences between cybersecurity-related concepts such as cyberattacks, cyberwarfare, hacktivism, and cyberterrorism. According to Kenney (2014), these concepts share many similarities making it difficult to differentiate among them. Under these concepts, the confidentiality, integrity, and availability of information systems are attacked using similar strategies, while external attributes may be different.

External attributes. Kadivar (2014) performed a literature review and used expert advice to identify common attributes across the definitions of cyberattacks. In the study, five attributes constituting cybersecurity were identified, including actors, assets, motivation, effects, and duration. Fok (2015) also used literature review and identified similar attributes affecting cybersecurity. According to Fok (2015), actors include individuals, organized groups, and nation states. The first group includes hackers, amateurs, script kiddies, and people with technical skills looking for "fun or notoriety" (Fok, 2015, p. 33). The second groups mixed insider threats and organized groups like criminal organizations and hacktivist. The third group includes "terrorist and nation states engaged in cyber warfare" (Fok, 2015, p. 33).

According to a recent report by the Office of the Director of National Intelligence (2017), Russia as a nation-state performed a cyber intrusion on multiple state and local electoral boards systems. Other potential targets consist of different information systems and data assets, including critical infrastructure. Miron and Muita (2014) used a literature review to study cybersecurity capability maturity models relevant to improving the security posture of critical infrastructure providers. Critical infrastructures are "assets or systems required for the security and well-being of citizens" (Miron & Muita, 2014, p. 33). These systems support and provide "energy, transportation, telecommunication, water supply and waste management, agriculture and food supply, finance, public health, and essential government services" (Hua & Bapna, 2013, p. 175). On the other hand, motivations can consist of individual beliefs or shared ideals that could be influenced by economic, political, and social factors. The effects of a cyberattack can include

"alteration, deletion, corruption, deception, degradation, disablement, disruption, or destruction of assets" (Kadivar, 2014, p. 23).

Economic. According to Kadivar (2014), the government, the private sector, and academia are aware of the high cost related to cyberattacks and vulnerabilities management. The public and private sectors are reducing operational cost through automation and system integration. On the other hand, these sectors had increased their yearly spending on cybersecurity (Clinton, 2015). The private sector is spending more than "$100 billion", while the federal government spends less than "$15 billion" (Clinton, 2015, p. 55). These investments can result in a major challenge for most government agencies, particularly those with small populations (Saxby, 2015).

Cyberattacks can force the deviation of government funds from public services to respond and recovery efforts related to the attack (Hua & Bapna, 2013). For instance, a cyberattack against the Departamento de Hacienda de Puerto Rico (Hacienda) [Department of Treasury of Puerto Rico] had a cost of $30 million per day (Minelli-Pérez, 2017). The online tax payment system was unavailable for five days preventing the submission of 46,000 individual tax records and payments, thus causing a significant impact on government revenues (Tellado-Domenech, 2017). Responding and recovering from a cyberattack can lead to unanticipated expenditure resulting in a decrease of government service, budget deficit, and the need to increase taxes.

Political. Rowland, Rice, and Shenoi (2014) conducted a literature review to explain the concepts of cyber power, its components, and characteristics, as well as their importance in achieving and maintaining power. Cyberspace is a relatively new domain

that offers “speed and reach, anonymity and protection, and the ability to create and participate in virtual economies” (Rowland et al., 2014, p. 3). The ideologies of a cyber state include the concept of *digital citizenship* where e-government and e-economy models are used to satisfy their social contract supporting the economy and social stability, as well as to provide services related health, education, and public safety, among other elements (Rowland et al., 2014).

Saxby (2015) used a seminar composed of presentations “followed by a panel-based question and answer session” (p. 164) to explore the meaning of digital citizen and its implication on policy. Internet technologies are providing the means to bridge the communication gap between the government and its constituents (Saxby, 2015). Digital citizenship encompasses a sense of community, right to participate, and the commitment to take part in civic matters. However, recent incents such as Russia’s cyber intrusion on state and local systems can affect people trust on these digital platforms (Office of the Director of National Intelligence, 2017).

The Government of Puerto Rico uses Internet technologies to facilitate the delivery of public services. For instance, Hacienda uses information systems to manage lottery and tax services. Recently, this agency was the target of a cyberattack, and PII from taxpayers could have been compromised as part of the cyber incident (Minelli-Pérez, 2017). Elmaghraby and Losavio (2014) stressed the importance of using “legal and technical security measures” (p. 496) to preserve confidentially and privacy. For these reasons, Saxby (2015) identified cybersecurity as a critical element in provisioning government services and supporting the concept of a cyber state.

Social. Cybersecurity is a societal concern like public safety (Elmaghraby & Losavio, 2014; Levesque, Walsh, & Whyte, 2015). Elmaghraby and Losavio (2014) used literature review to examine cybersecurity challenges in smart cities. The concept of *smart cities* expands on the idea of digital citizens by benefiting from new technology, including "energy meters, security devices, smart appliances," among other devices (Elmaghraby & Losavio, 2014, p. 491). These systems support public services, including water, sanitation, emergency response, and disaster recovery (Elmaghraby & Losavio, 2014). According to Kenney (2014), the United States is the target of "hundreds of thousands of cyberattacks," (p. 112) especially against the Supervisory Control and Data Acquisition (SCADA) systems supporting critical infrastructure.

Hiller and Russell (2013) performed a literature review to explore the cybersecurity conditions, approaches, and legal framework used in the United States and the European Union. According to the study, "25% of all power companies globally have been hacked by cybercriminals" (Hiller & Russell, 2013, p. 237). In early 2000, a SCADA system was attacked in Australia resulting in the "release 800,000 gallons of raw sewage into adjacent rivers, parks and the grounds of a nearby hotel, destroying marine life and creating a nauseating stench for local residents" (Kenney, 2014, p.124). Similar attacks against SCADA systems have occurred in other countries such as Azerbaijan, Germany, Georgia, and Turkey (Levesque et al., 2015).

Influence of Institutional Frameworks on Cybersecurity

The institutional framework serves a legal framework covering policies, directly and indirectly, related to cybersecurity. The primary concern with this dimension is the

absence of policies covering technology (Picazo-Vela et al., 2012). According to Bertot et al.' (2015) literature review of information security policy and governance, "the legal structures, frameworks, authorization, and powers regarding national and international security" (p. 105) are continuously evolving. Tehrani et al. (2013) took advantage of case studies to examine the jurisdictional aspect of cybersecurity. Based on the study, Tehrani et al. affirmed that cybercrime could not be prevented, but it can be deterred through legal frameworks and prosecution. Information security policies are essential to provide a legal framework capable of safeguard organization, nations, and international boundaries.

Government agencies are ruled by the laws and regulations establishing their mission and defining the context of their operational environment. Therefore, policies can serve as a vehicle to influence the cybersecurity posture of government agencies. FISMA of 2014 is the primary law defining the cybersecurity requirements and mandating compliance with "related policies, procedures, standards, and guidelines" (p. 128). This statue gives regulatory power to OMB which exercises its responsibility in the form of circulars, memorandums, and defined reporting mechanism. Further, FISMA of 2014 assigns NIST the responsibility of developing guidelines in the form of Special Publications (SP) and Federal Information Processing Standard (FIPS) to safeguard the confidentiality, integrity, and availability of national systems. However, these policies are not mandated outside the federal government.

Local governments are "creatures of the states" (Levy, 2012, p. 68) receiving their mandates and much of their funding from the state government. E-Government Act of 2004 is the primary law driving the use of IT to promote e-governance in Puerto Rico.

The key objectives of this Act are represented in Figure 3. The pyramid shows the interrelationship of the E-Government Act of 2004 objectives acting as building blocks leading to empower citizens to be able and capable of participating in the different aspects of democratic governance. The law requires these objectives to be achieved while ensuring the protection of privacy, security, and availability of the information. Therefore, the principles of cybersecurity serve as the foundation supporting all e-government goals and objectives. Like FISMA of 2014, the E-Government Act of 2004 mandates OGP to coordinate access to information and government services with all agencies. Moreover, OGP is responsible for developing and establishing policies and guidelines for the protection of privacy and cybersecurity. The E-Government Act of 2004 uses a similar policy framework as FISMA of 2014 by including circulars, memorandums, and guidelines.

Roesener et al. (2014) performed a qualitative study of information security policy in the United States to understand the different roles, responsibilities, and authorities influencing the national cybersecurity posture. Roesener et al. found that the roles and responsibilities of government agencies are overlapping and lacking authority to make decisions (Roesener et al., 2014). Similarly, the E-Government Act of 2004 is considered vague, especially regarding the role and responsibility of government agencies to support e-government (Certificates and Electronic Receipts Act; 3 L.P.R.A. § 8721). The vagueness of the law resulted in the development and enactment of additional legislation to cover the gaps. OGP developed an ongoing series of policies known as TIG to provide additional guidance to fulfill the mandate of the E-Government Act of 2004.

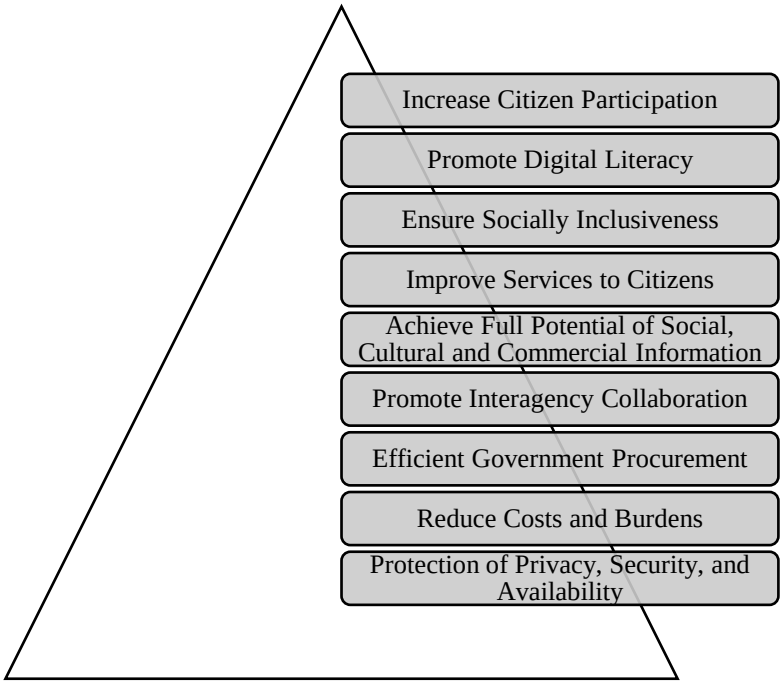

Figure 3. Puerto Rico's e-government goals. Adapted from the E-Government Act of 2004, 3 L.P.R.A. § 991 (2004).

The TIG-003, *Security of Information Systems* is the foundation supporting the cybersecurity posture of government agencies in Puerto Rico. This policy established the general guidelines to facilitate the implementation of security controls by government agencies and support the confidentiality, integrity, and availability of information systems and data assets under their jurisdiction. According to TIG-003, security is an integral part of the system design. However, the policy does not mention audits, timelines, or processes to review compliance at the municipal level.

In 2016, 12 years after the implementation of TIG-003 the Office of the Comptroller of Puerto Rico issued a circular (OC-16-16) to evaluate the security controls implemented in municipal information systems. TIG-003 introduced several critical aspects supporting cybersecurity that are aligned with the elements of this research and

are discussed in more detail under other TIGs. Appendix A: Cybersecurity Dimensions Covered by TIGs shows some of the cybersecurity elements covered by TIGs. Kazemi et al. (2012) used a mixed method case study to evaluate the success factors related to municipal information security programs. Kazemi et al. identified compliance with security standards as an important factor for the successful implementation of information security programs. Nevertheless, most of the TIG series failed to reference government and industry standards, as well as to provide detailed guidance.

Executive orders have also played a significant role within the institutional frameworks supporting the cybersecurity posture of government agencies in Puerto Rico. Before the enactment of the E-government Act of 2004, the government used Executive Order OE-2000-019 to establish CIOs at the agency level. However, Executive Order OE-2000-019 did not create a central office for managing standards, compliance, or guidance to help the new CIOs in managing their information resources in a uniform and secure manner. This situation led to incompatibilities among agencies information systems causing roadblocks, duplicative efforts, and costly solutions. Further, these conditions affected the transferability and availability of data among agencies to improve the management and delivery of public services.

In 2009, OE-2009-009 was passed establishing the role of the CIO of Puerto Rico and the Oficina del Principal Ejecutivo de Información del Gobierno de Puerto Rico [Office of the Chief Information Officer (OCIO) of Puerto Rico]. The primary responsibilities of the CIO were advising the governor and acting as the governor's representative in all IT-related matters. The order made OCIO responsible for performing

accountability of all government information systems to facilitate system integration; identifying and reducing duplicative efforts; lowering operational cost and improving public services. OCIO was also mandated to develop, implement, and publish policies, standards, and best practices to protect government systems from cyber threats. The office had a dedicated budget and the ability to manage federal, state, and local funds.

During 2015, Executive Order OE-2015-019 (2015) was ratified to repeal Executive Order OE-2009-009 (2009). The order recognized the success of the OCIO in fulfilling their mandates. Nevertheless, Executive Order OE-2015-019 (2015) eliminated the role of the CIO of Puerto Rico, dismantled the OCIO, and reassigned its duties to the DDEC. The executive order was justified from the perspective of economic development and did not consider the impact on public administration and management of government systems. On January 2017, the newly elected administration used an executive order to reestablish the OCIO under the name of Servicio de Tecnología de Innovación de Puerto Rico [Technology and Innovation Service of Puerto Rico].

Influence of Interorganizational Collaboration on Cybersecurity

The interorganizational dimension covers the collaboration and networking efforts that interact with external organizations within the government and private sector (Picazo-Vela et al., 2012). The interconnectivity of information systems continues to have a transformational impact on public safety, critical infrastructure, global commerce, and access to near real-time data (Hiller & Russell, 2013; Levesque et al., 2015; Lozowski, 2014). However, the complexity of interconnection requires the government to go beyond securing their systems and helping safeguard interconnected systems. Scholars

agree that the government alone cannot secure cyberspace and needs the support and collaboration of other sectors (Clinton, 2015; Hiller & Russell, 2013; Hua & Bapna, 2013; Miron & Muita, 2014; Roesener et al., 2014).

Unfortunately, government agencies tend to act independently and fail to take into consideration what is being done by other entities (Gil-Garcia & Pardo, 2005). Manley (2015) reviewed secondary data, including previous studies, surveys, and interviews related to cybersecurity and PPPs. Manley (2015) explained that government officials such as former U.S. President Obama and former CIA Director Panetta recognized the importance of PPP to improve the national cybersecurity posture. Early policy efforts such as the Presidential Decision Directive 63 had also recognized the importance of public and private collaboration as part of a national cybersecurity framework (Hiller & Russell, 2013).

More recent policy efforts like the 2009's Comprehensive National Cybersecurity Initiative included increasing cooperation between "federal, state, local and private sector actors," (Hiller & Russell, 2013, p. 239) supported education and research and defined clearer roles among partners. Similarly, HSPD 7: Critical Infrastructure Identification, Prioritization, and Protection and its successor PPD-21: Critical Infrastructure Security and Resilience promoted collaboration among the industry, the research community, and government agencies, including state and local governments (Roesener et al., 2014). The Government of Puerto Rico has also encouraged interorganizational collaboration through legislation such as the E-Government Act of 2004 and related policies. The

deprecated OE-2009-009 gave the OCIO of Puerto Rico the responsibilities for IT-related interorganizational collaboration with municipal, state, and federal agencies.

Clinton (2015) used case studies to analyze the strategies related to the success and failure of PPPs. Policy can be used as a strategy to require government agencies to work collectively with the private sector, especially "to identify industry-based standards and practices worthy of voluntary adoption" (Clinton, 2015, p. 56). Yusta et al. (as cited by Miron & Muita, 2014) mentioned that "standards bodies and federal agencies in at least 12 countries or regions have defined criteria for security standards as well as implementation methods" (p. 34) to lessen the complexity of risk management. PPPs can help to achieve "a common lexicon for categorizing and managing cyber risks" that could facilitate "a common understanding around various risk management terms, methodologies, ideas, and language" (Clinton, 2015, p. 67).

Department of Homeland Security and Carnegie Mellon University are an example of a PPP promoting advancement in cybersecurity through "workforce development, process maturity, and operational resilience" (Miron & Muita, 2014, p. 36). Similarly, municipalities could establish partnerships with local universities. Kostyuk (2014) used a case study to understand challenges related to cybersecurity and explore cooperation as a strategy to address them. Based on the study, small public agencies such as municipalities should partner with other organizations to strengthen their capabilities and collectively improve their cybersecurity posture (Kostyuk, 2014).

Collaboration can help improve problem-solving and public services through knowledge and best practice sharing (Picazo-Vela et al., 2012). Furthermore,

interorganizational collaboration can take place at all levels from municipal to international organizations. Tehrani et al. (2013) used literature review to study cyberattacks such as cyberterrorism from a multijurisdictional perspective. Since cyberattacks can occur across borders, there is a need for a global response. At the international level, the International Telecommunication Union (ITU) and the International Criminal Police Organization (Interpol) sponsored the International Multilateral Partnership against Cyber Threats (IMPACT) which became "the world's first global PPP against cyber threats" (Tehrani et al., 2013, p. 214). This alliance includes 191 countries collaborating and sharing threats "against the global financial system, power grids, nuclear plants, and air traffic control systems" (p. 214).

Douba, Rütten, Scheidl, Soble, and Walsh (2014) linked a transdisciplinary model with the prospect theory as a strategy to support risk-based decision making to explore the concept of online safety, its impact, and possible approaches to addressing related concerns. According to Douba et al. (2014), collaboration must occur across different levels. Practical solutions must account for the value level, which encompasses "theology, values, security and privacy, intellectual property, regulation, disclosure, and the individual and collective good" (Douba et al., p. 43, 2014). On the other hand, the normative level consists of "risk-based decision-making, management and planning, the strategy for making scientific progress and knowledge sharing, legal, and political concerns" (Douba et al., p. 43, 2014). The 2011's U.S. International Strategy for Cyberspace included collaboration in similar areas to facilitate "1) establishing risk-based security practices, 2) information sharing, 3) adopting international technical security

standards for products and services" (Hiller & Russell, 2013, p. 239). PPPs should serve as a model for interorganizational collaboration on cybersecurity that can be implemented throughout different government level, including municipalities.

Influence of Organizational Structures and Processes on Cybersecurity

The organizational dimension includes the impact of structures and processes on the organization's performance (Picazo-Vela et al., 2012). Bertot et al. (2015) described prevention and response as critical cybersecurity processes. The former allows organizations to manage risk before it happens while the later gives organizations the ability to react. The capabilities to prevent and respond to cyber threats are directly related to the organization's structures, resources, technologies, and policies.

Organizational structures. On a centralized structure, the body of governance is responsible for cybersecurity processes such as managing controls, awareness, and training. On the contrary, under a decentralized structure, these responsibilities fall under individuals or small groups with limited resources. Armbruster, Endicott-Popovskyb, and Whittington (2013) used a case study to investigate the impact of aging infrastructure on municipal systems. Armbruster et al. (2013) discovered that the development of standards, the adoption methodologies, and the implementation of best practices is more challenging for decentralized IT departments.

Moreover, Flores, Antonsen, and Ekstedt (2013) used a mixed methods research including literature review and surveys to collect data from 578 information security executives within the United States and Sweden. According to a recent study by Flores et al. (2013), centralization is more efficient to achieve uniform guidance and facilitate

information sharing. The way the organization interacts is also crucial in supporting cybersecurity. Manley (2015) explained that implementing a bottom-up approach is fundamental to fulfilling legal requirements and support collaboration. Previous investigation has shown that the use of a top-down approach placed more attention on the organization at the top while a bottom-up approach gives "autonomy to react quicker to cyberattacks, thus being more resilient" (Manley, 2015, p. 95).

The people, their roles, and their responsibilities are also essential elements of the organizational structure. Kazemi et al. (2012) identified seven organizational factors required for the successful implementation of an information security program at the municipal level. These factors are "top management support, information security policy, job responsibilities, the motivation of the employees, awareness and training programs, compliance with information security international standards, and using the services of the information security external advisors" (p. 4982). Reece and Stahl (2015) performed a qualitative study to examine cybersecurity as a profession and investigated the perspectives of practitioners on the profession. Reece and Stahl identified the need for top management to include the role of a cybersecurity executive such as a chief information security officer (CISO) with the responsibility of incorporating cybersecurity as part of the enterprise governance (Reece & Stahl, 2015). The CISO or IT leaders with cybersecurity responsibilities must understand the organizational culture as part of policy development and implementation (Flores et al., 2013; Kazemi et al., 2012). For instance, organizations, where employees are hesitant to take ownership of cybersecurity efforts,

there must be defined roles and responsibilities. A lesson learned after the cyberattack against Hacienda was the lack of a CISO role in the agency(Minelli-Pérez, 2017).

Kazemi et al. (2012) mentioned the importance of employee motivation to support cybersecurity. IT professionals are constantly defending their organizations from cyberattacks, but their roles are not considered heroic. Nugent and Collar (2015) affirmed that it is hard to differentiate their heroism versus the perception that the IT professionals are just performing their job. This situation can negatively impact the motivation of employees and the attractiveness of the career for new practitioners. The demand for cybersecurity professionals is over three times greater than the offer (Levesque et al., 2015; Reece & Stahl, 2015). IT leaders can take advantage of organizational heroes to create a positive effect on job satisfaction. With the continuous increase in cyber threats, it is important to maintain job attractiveness for the current and upcoming workforce.

Organizational processes. Elmaghraby and Losavio (2014) used a combination of literature, a paradigm developed by IBM, and the routine activities theory to examine the relationship and challenges of cybersecurity in smart cities. According to the routine activity theory, identifying suitable targets can lead to the development of technical, operational, and administrative controls and processes to serve as capable guardians for deterring attackers and preventing the success of their actions (Elmaghraby & Losavio, 2014). For these reasons, security controls must include processes for "prevention, detection, and recovery" (Elmaghraby & Losavio, 2014, p. 496). Kazemi et al. (2012) described information security programs as an iterative process, requiring "feedback and continuous improvement" (p. 4984) to reduce the risks originating from cyber threats.

Further, the process requires prevention and detection elements such as identifying security controls and assessing their effectiveness.

Organizations rely on frameworks, standards, and best practices to model their security programs. However, a blanket implementation of these frameworks fails to place "attention to the differences between organizations and their information security requirements" (Flores et al., 2013, p. 91). For instance, municipalities often serve as critical infrastructure providers and are subject to numerous security controls and standards (Miron & Muita, 2014). Furthermore, Rogers (as cited by Miron & Muita, 2014) mentioned that organizations like municipalities could "be seen as laggards" (p. 37) on adopting standards. Kazemi et al. (2012) explained that smaller organizations face significant challenges due to their lack of resources.

The implementation of security controls, standards, frameworks, and best practices are complex, costly, and time-consuming process (Miron & Muita, 2014). Hua and Bapna (2013) reviewed current literature about "cyber terrorism, terrorism deterrence, IS security investment, and prior studies on game theoretical models" (p. 176) to explore key factors affecting cybersecurity investment. Hua and Bapna said that cost-effective investments could improve resiliency, reduce risk, and potential negative impact on the organization's systems and reputation. For example, subsidizing cybersecurity investments, certifying compliance, performing periodic audits, and sharing lessons learned can be used by the government to improve their cybersecurity posture. Nevertheless, budget constraints can influence the procurement of IT services based on cost rather than best value (Armbruster et al., 2013).

Another important factor to consider is the organizational process for remediating vulnerabilities. Controls such as "policies and procedures for security, technical solutions, and contracts with suppliers, service providers, and customers" (Hiller & Russell, 2013, p. 237) are essential to mitigate vulnerabilities. Hua and Bapna (2013) stressed the importance of addressing technical and administrative vulnerabilities to increase the effectiveness of cybersecurity investments. Asset management is a crucial element in vulnerability management. Asset management includes the procedures for conducting inventory on municipal assets, allocation of resources, capital planning, and the forecasting of resources and requirements while complying with pertinent regulations (Armbruster et al., 2013). Unfortunately, asset management could be constrained by the absence of the resources to support the process.

Influence of Information and Data on Cybersecurity

The information and data dimension encompass elements such as availability, integrity, completeness, and quality of data assets (Picazo-Vela et al., 2012). The lack of high-quality data was a contributing factor affecting IT projects. Similarly, information and data deficiency could have an impact on cybersecurity operations. Cybersecurity is "a human-centered process, fully informed by both technical and social aspects" (Reece & Stahl, 2015, p. 182). For this reason, attackers are concentrating on social components over technical vulnerabilities (Flores et al., 2013). Adams and Makramalla (2015) explored gamification and entrepreneurial perspectives as strategies to strength awareness training and improve resiliency against human exploits. As part of their literature review, Adams and Makramalla highlighted recent studies showing that 80% of cybersecurity

exploits are related to the human element. Therefore, it is critical to consider the accessibility, availability, and completeness of the data needed to help end users and IT professionals secure their organizations and improve their cybersecurity posture.

According to a recent report, 24% of participants stated that the effectiveness of their organizations in dealing with cyber incidents has declined (Lozowski, 2015). Scholars agree that most security programs lack the methodology and empirical data to measure their effectiveness (Flores et al., 2013). The lack of empirical data affects the ability of IT leaders to understand and improve the cybersecurity posture of their organizations. Methodologies such as such cybersecurity capability maturity models can be used for measuring hierarchical progress related to “conditions, processes, or application targets” (Miron & Muita, 2014, p. 36). These measurements can capture historical performance data in alignment with defined maturity levels. This information can then be used to support the development of strategies to move the organization into a more desirable state.

Douba et al. (2014) affirmed that there is a relationship between digital literacy and cyber resiliency. Unfortunately, there is limited access to “highly qualified personnel” (Levesque et al., 2015, p. 29) with an appropriate level of cybersecurity knowledge and experience. Personnel without an appropriate level of expertise could have an adverse impact on their organization’s security posture. Insiders with legitimate "access to an organization’s information or information systems” (Posey, Roberts, Lowry, & Hightower, 2014, p. 551) can commit inadvertent actions such as unintentionally activate a malicious payload.

The cyberattack against Hacienda used a human exploit strategy know as ransomware where someone internal inadvertently clicked on a malicious payload that encrypted a portion of the agency's data assets prohibiting access to the systems and data (Tellado-Domenech, 2017). Chen and Dongre (2014) performed a qualitative study to understand the motives of attackers to develop better controls to protect systems. In addition to inadvertent actions, insiders can have motives to deliberately commit actions with malicious intent (Chen & Dongre, 2014). One of the most dangerous actions is inaction. According to a recent study, 54% of data compromises occurred during 2013 were related to negligence (Adams & Makramalla, 2015).

Douba et al. (2014) identified seven knowledge domains that are necessary for online safety, including knowledge transfer or information sharing. Information sharing supports advancement in "cybersecurity tools and techniques" (Levesque et al., 2015, p. 30). Information sharing is the distribution of information to facilitate collaboration, problem-solving, innovation, and implementation of governance (Flores et al., 2013). Flores et al. (2013) revealed that the participants in their study affirmed coordination of security activities affects information sharing, particularly related to "risk management and performance monitoring" (p. 97).

Conducting security assessments requires the coordination of security activities. For instance, the vulnerabilities discovered during security assessments must be shared with the proper personnel for remediation. Failure to properly communicate these findings can place the organization at risk of cyberattacks. Muegge and Craigen (2015) used a combination of secondary data, conversations with practitioners, and the

perceptions of graduate students within a design science approach for developing a process for improving the quality and dissemination of risk data. Muegge and Craigen affirmed that elements such as “secrecy, competition, and public image” (Muegge & Craigen, 2015) serve as deterring factors to information sharing affecting the organization’s ability to learn, manage, and mitigate cyber threats.

PricewaterhouseCoopers reported that the annual losses of organizations without cybersecurity awareness training reported an average of 76% higher losses than those organizations that provided training (Adams & Makramalla, 2015). Posey et al. (2014) conducted qualitative semistructured interviews with 33 participants, including 11 insiders and 22 security professionals from different organizations within the United States to compare their perceptions on cybersecurity-related matters. The findings make of security education, training, and awareness (SETA) programs an essential part of the organization’s security program (Posey et al., 2014). The use of appropriate awareness training could have served as a mitigation control to deter the success of the cyberattack against Hacienda. Nevertheless, awareness training alone does not provide adequate means to develop the necessary skills to protect organizations (Adams & Makramalla, 2015; Reece & Stahl, 2015). Strategies such as gamification facilitate information dissemination and understanding allowing participants to increase their skills to prevent and mitigate cyber threats (Adams & Makramalla, 2015). Employees should have a clear understanding of the organization’s cybersecurity goals and “that security is everybody’s job” (Posey et al., 2014, p. 565).

Influence of Technology on Cybersecurity

The technology dimension consists of information systems components, as well as their compatibility, usage, and management (Picazo-Vela et al., 2012, p.107). Technology represents both threats and opportunities. Levesque et al. (2015) completed a qualitative study on the challenges inhibiting cybersecurity. According to Levesque et al., complexity is a key factor affecting cybersecurity. Cisco projected a total of 50 billion devices connected to the Internet by 2020 (Levesque et al., 2015). The increase in systems interconnectivity introduces "new vulnerabilities, adversarial threats, and challenges" (Levesque et al., 2015, p. 26) affecting the security of the systems and related data. Further, technology gives attackers the ability to target information systems from anywhere in the world. Failing to understand these challenges and adapt to new technologies could have adverse effects on government operations and their constituents.

On the other hand, new technologies also represent opportunities to manage, mitigate, prevent, and respond to cyber threats. Levesque et al. (2015) identified seven factors to improve the cybersecurity posture of organizations, three of which were related to the use of cybersecurity-related technologies. The use of antivirus, firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), among other security appliances, is essential to prevent and respond to cyberattacks (Hua & Bapna, 2013; Levesque et al., 2015). Furthermore, the implementation of systems capable of automatically responding to cyberattacks without human interaction is crucial to improving the organization's cybersecurity posture (Kostyuk, 2014; Levesque et al., 2015). For instance, an IDS is only capable of detection and notification, while an IPS

can apply learned patterns and analysis to respond to cyberattacks automatically. According to a recent report, Russia access to state and local system since 2014 was discovered by U.S. intelligence instead of the people responsible for the systems (Office of the Director of National Intelligence, 2017). The use of cybersecurity technology solutions can help to identify and prevent cyber intrusion.

These technologies are expensive and could require hiring personnel with specialized capabilities or reeducate the current staff. However, the effect of cyberattacks against government institutions could be even more costly. For instance, the impact of the recent cyberattack against Hacienda has been estimated to cost over $30 million without counting the recovery and remediation efforts (Minelli-Pérez, 2017). Maheux (2014) merged an intention-based classification of malware and an optimal timing model as a tool to "help predict the timing of malware based on its classification" (p. 34). Maheux (2014), emphasized a recent report by Symantec explaining that the annual impact of cybercrime exceeds $110 billion and affects 566 million victims. Kadivar (2014) examined 10 high-profile cyberattacks and identified six attributes in common, including vector, vulnerability, malicious software, botnet reliance, origin, and destination. The attack vector is the entry point to commit "the exploitation" (Kadivar, 2014, p. 24). Malicious software or malware includes the "viruses, worms, trojan horses, and spyware" (Maheux, 2014, p. 34) used to commit cyberattacks. Ransomware was the malware used on the cyberattack against Hacienda. This type of malware encrypts data assets and request payment to decrypt the data and regain access to the information.

These technologies have continued to improve their capability to bypass detection, replicate, and open covert channels to establish command and control (Hua & Bapna, 2013). Zeus is an example of malware stealth to antiviruses that compromised over 74,000 accounts in 2007 from "Bank of America, NASA, Monster.com, ABC, Oracle, Cisco, Amazon, and BusinessWeek" (Maheux, 2014, p. 35) causing economic losses of over $70 million. Maheux (2014) merged an intention-based classification of malware and an optimal timing model as a tool to "help predict the timing of malware based on its classification" (p. 34). In the case of the cyberattack against Hacienda, this timing of malware could have helped predict that an agency responsible for collecting taxes have a higher probability to be attacked during tax season. Understanding the relationship between the timing, categorization, and intention of malware can improve the ability to defend information systems resources and data assets.

Sá et al. (2015) used convenience sampling to identify 25 participants for a 20-minute questionnaire about local e-government. Sá et al. explained that e-government consists of the implementation of technological solutions to enable communication and services with internal and external parties such as constituents, other government agencies, and the private sector. This approach has increased the government's dependency on "energy and computing infrastructures" (Armbruster et al., 2013, p.123) to support e-government and e-democracy. Armbruster et al. (2013) used a case study approach to explore the impact of a cyber incident related to aging infrastructure and raised awareness on the importance of protecting critical systems. Based on the study, Armbruster et al. recommend hosting data centers with appropriate infrastructure and

avoid “repurposing buildings that were not intended to accommodate the requirements of critical computing infrastructures” (p. 124).

Information systems must be resilient to human-made and natural disasters. Therefore, government agencies need to identify contingency strategies to support their critical systems and operations. A recent survey showed that out 71% of organizations with tested business continuity plans, half reported: “technical, equipment, logistical or management problems during an exercise” (Armbruster et al., 2013, p. 125). During the attack against Hacienda, it was discovered that contingency planning and testing was not performed contributing to the loss of 50 terabytes of data because of the attack (Minelli-Pérez, 2017). Developing and managing contingency plans can be costly and difficult for government agencies to maintain after budget cuts. Cloud services can also facilitate disaster recovery and continuity of operations, improving the resilience of systems and processes. The U.S. General Services Administration is leading an initiative to consolidate 40% of the federal agencies’ data centers to reduce operational costs and facilitate technical improvements.

Summary and Conclusions

The literature surrounding cybersecurity has continued to expand and contribute to the body of knowledge. However, research attention continues to focus on cybersecurity at the national and international level. Local governments use the same data types to fulfill their mandates as first responders, critical infrastructure providers, and enablers for social and economic development within their jurisdiction (Miron & Muita, 2014; Sylves, 2015). These data assets reside within cyberspace and depend on

interconnectivity to other systems. Attacks against these information resources can adversely affect the operations of the targeted, as well as the interconnected systems. These conditions should drive more attention toward cybersecurity at the local level.

The literature search strategy concentrated on the research problem and not in the conceptual framework. However, the major themes found during the literature review were in alignment with the dimensions influencing digital government. Also, most of the literature was consistent with themes within the predefined dimensions. For instance, the elements captured within the general context dimensions included economic, political, and social factors. These factors played a significant role in understanding cyberattack attributes such as objectives, actors, and targets (Fok, 2015; Kadivar, 2014; Kenney, 2014). Regarding the institutional framework, the literature supports the need for standards and information security policies (Armbruster et al., 2013; Clinton, 2015; Flores et al., 2013; Hiller & Russell, 2013; Kazemi et al., 2012; Miron & Muita, 2014; Picazo-Vela et al., 2012; Tehrani et al., 2013).

System interconnectivity and limited resources were major themes under interorganizational collaboration and networks. As technology continues to evolve, more systems are interconnected. This characteristic improves productivity but expands the surface of attack to include vulnerabilities in the interconnections and the interconnected systems (Hiller & Russell, 2013; Levesque et al., 2015; Lozowski, 2014). On the other hand, interorganizational collaboration can improve problem-solving, reduce administrative overhead, and benefit from the strength of other organizations to collectively improve cybersecurity (Flores et al., 2013; Picazo-Vela et al. (2012). The

literature favored the use of centralized organizational structures and bottom-up communication for achieving and supporting a resilient cybersecurity posture (Armbruster et al., 2013; Flores et al., 2013; Manley, 2015). Most of the organizational processes found during the literature review were related to the concepts of prevention, detection, and recovery (Elmaghraby & Losavio, 2014; Kazemi et al., 2012).

The literature also supported the importance of information and data in achieving a resilient cybersecurity posture. Information about the security policies, cyber threats, and mitigation strategies needs to be available, accessible and well disseminated (Douba et al., 2014; Flores et al., 2013; Hiller & Russell, 2013; Levesque et al., 2015; Muegge & Craigen, 2015). Similarly, technology must be available, procured, and properly configured. Scholars agree on the importance of the implementation of cybersecurity-related technologies, especially those capable of automatically responding to cyberattacks without human interaction (Hua & Bapna, 2013; Kostyuk, 2014; Levesque et al., 2015).

Most of the literature concentrated on identifying missing technical, operational, and administrative controls, and providing possible solutions to improve cybersecurity. For instance, information security policies, collaboration, cybersecurity processes, information sharing, awareness and training, and cybersecurity-related technologies were some of the controls identified in literature needing to be developed, implemented, or improved to achieve a resilient posture. However, the literature did not explore why these security controls were not present or why these possible solutions were not implemented in the first place. Understanding what is affecting the local government's ability to achieve a resilient cybersecurity posture could help to identify the groundwork required

to upkeep the development and implementations of cybersecurity controls which consequentially could improve and maintain their posture.

This study could contribute to the resolution of two major gaps in the literature. The first gap is the absence of cybersecurity research outside a national and international context. This study provided research-based data on the cybersecurity posture of local governments. The second gap is related to the factors affecting the development and implementation of security controls. The literature contained evidence of the use of security controls to improve cybersecurity. However, the literature lacked focus on the challenges and factors affecting the adoption of such security controls. Understanding these factors is essential for the development of cost-effective solutions that are suitable for each local government agency. These contributions could extend knowledge in public policy, public administration, and IT management.

The following chapter describes the research methods for this study. The research methodology is in alignment with the gap discovered during the literature review. A significant portion of the literature was solely based on a literature review with no additional connection to participants. Several researchers took advantage of case studies, interviews, and expert advice as part of their methodology. Based on the significant gap in literature and knowledge about cybersecurity at the local government level, a qualitative phenomenological approach could be crucial to extend knowledge in the discipline by studying information-rich cases to collect as much data as possible about the phenomenon. Chapter 3 included detailed descriptions of the research design, the researcher's role, methodology, and strategies to address potential trustworthiness issues.

Chapter 3: Research Method

The research design for this study facilitated the understanding of the cybersecurity posture of municipalities in Puerto Rico. This phenomenon involved the readiness of municipal governments' "networks, information, and systems based on IA resources (e.g., people, processes, technologies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes" (Kissel, 2013, p. 179). Furthermore, this study addressed key factors influencing the cybersecurity posture of municipalities. The outcomes of this investigation may help to improve the cybersecurity of government agencies in Puerto Rico by providing advances in knowledge that could support the development of administrative, operational, and technical controls.

Phenomenology was the qualitative design used to conduct the study. This design is used to explore the human experience with the phenomenon (Moustakas, 1994). The study included a transcendental approach to concentrate on the essence of the experiences of IT leaders. The understanding of the phenomenon and related elements was gained through the perceptions of public servants leading IT efforts at the municipal level. A sample of this population was drawn from settings consisting of highly populated municipalities within the San Juan – Carolina – Caguas MSA.

This chapter includes the rationale for the research design, the role of the researcher, the methodology, and issues related to trustworthiness. The design rationale includes the reasoning for using transcendental phenomenology for the study. Bracketing was used to explain my experience with the phenomenon and manage biases. The methodology section includes comprehensive details about the selection of participants,

the research instrument, data collection, and data analysis. Also, this chapter addresses ethical concerns and mitigation strategies to support the trustworthiness of the study.

Research Design and Rationale

The research questions supported the purpose of the study and indicated the appropriate method for conducting the study. A combination of two qualitative research questions guided this study. These research questions addressed the perceptions of IT leaders concerning their lived experiences with cybersecurity:

RQ1: How do public servants in IT leadership roles perceive the cybersecurity posture of government municipalities in Puerto Rico?

RQ2: What factors do public servants in IT leadership roles perceive as most influential to achieve a resilient cybersecurity posture in government municipalities in Puerto Rico?

The central question of the study was RQ1. This question was used to understand the readiness of government municipalities to protect and defend information resources. Although the primary research question could have resulted in a positive or negative understanding of the phenomenon, RQ2 focused on the elements influencing the understanding. This question was designed to provide a deeper understanding of the factors enabling or hindering public servants in protecting their information resources and data assets. Identifying and understanding influential factors are critical steps in developing strategies to stimulate conditions for improving cybersecurity and to mitigate those conditions preventing advances in its posture.

The central phenomenon of the study was the cybersecurity posture of the municipal government. The concept of cybersecurity relates to the capabilities required to safeguard information resources within cyberspace from cyber threats such as cyberattacks. Cyberattacks are intended to disrupt, disable, destroy, or control information resources, and to destroy data integrity or steal sensitive information (Kissel, 2013). The government's dependency on information resources has made cybersecurity a relevant phenomenon to study, especially as it relates to the posture of government agencies. The concept of security posture refers to the status of security controls in place by organizations such as municipal governments to manage and react to cyber incidents (Kissel, 2013). Failing to adopt a resilient cybersecurity posture can be detrimental to government systems, municipal governance, local economy, and public safety.

FOIA of 1966 safeguards most of the quantitative data related to cybersecurity from public disclosure. Cybersecurity data protected by FOIA of 1966 could include security assessments, audits, vulnerabilities, and security plans. Qualitative research provides the tools for understanding and "exploring the meaning individuals or groups ascribe to a social or human problem" (Creswell, 2013, Chapter 3: Summary, para. 1). Therefore, the insights of individuals can be used as reliable sources to study cybersecurity as a social problem. The research design for this study adhered to the characteristics of the qualitative research.

The five qualitative research traditions include narrative, phenomenological, grounded theory, ethnographic, and case study (Creswell, 2013). Each tradition provides a different scholarly structure for organizing and presenting ideas (Creswell, 2013). In the

current study, phenomenology provided the framework to substantiate the collection and analysis of data grounded in participants' experiences. The study centered on the experiences of public servants regarding cybersecurity in IT leadership roles at the municipal level. Using phenomenology as the research methodology enabled me to explore the research problem and capture the essence of the phenomenon.

Previous researchers have taken advantage of phenomenology to explore phenomena related to cybersecurity. Moore (2014) used phenomenology to explore the development of information security policies to safeguard national security and deter cybercrime. Heuristic and transcendental are the two major research approaches within the tradition of phenomenology. These approaches provide slightly different philosophies and frameworks. In the current study, transcendental phenomenology provided a suitable approach to address the research questions in alignment with the purpose.

Heuristic phenomenology requires researchers to "have personal experience and intense interest in the phenomenon" (Patton, 2002, Heuristic Inquiry, para. 2). In addition to the connection to the phenomenon, the heuristic approach emphasizes connecting with the participants. Moustakas (1994) explained that heuristic inquiry concentrates more on understanding the experience rather than the phenomenon. Heuristic phenomenology facilitates understanding of the phenomenon through "shared reflection and inquiry" (Patton, 2002, Heuristic Inquiry, para. 4). In traditional science, the characteristics of a heuristic approach can raise concerns regarding the objectivity of the researcher.

Transcendental phenomenology shares the heuristic principle of connectedness. Transcendental phenomenology also follows a "disciplined and systematic" (Moustakas,

1994, p. 21) approach. This approach includes a process known as *epoche* or *bracketing*. According to Moustakas (1994), bracketing gives researchers the means to set aside "prejudgments, biases, and preconceived ideas about things" (p. 21). As a professional, I had experienced the phenomenon of inquiry while performing in diverse roles at different government levels for 17 years. These experiences may have contributed to prejudgments, biases, and preconceived ideas about cybersecurity, especially as it relates to the posture of governments. The bracketing process supported the objectivity while sustaining the use of intuition, which was fundamental for the study.

Moustakas (1994) affirmed that reality is subject to the person perceiving it. Studying the perception of the reality of the cybersecurity posture of government municipalities depended on the lived experiences of the participants. This concept provided different insights into the phenomenon and the elements influencing it. In transcendental phenomenology, the process of converting empirical experience into essential insights is known as ideation (Moustakas, 1994). Through ideation, the consciousness of the participants is associated with the phenomenon creating meaning and extending the current body of knowledge. The previously discussed conditions supported the rationale of using transcendental phenomenology as the research design. Bracketing is further described in Chapter 4 as part of the evidence of trustworthiness.

Role of the Researcher

The researcher is the principal research tool for data collection in qualitative methods. Creswell (2013) explained that researchers could engage participants through different roles ranging from participatory to nonparticipatory. These roles include

complete participants, participants as observers, observers as participants, and complete observers. Depending on the role, researchers can take advantage of their sense of sight, hearing, touch, smell, and taste (Creswell, 2013). For this study, I adhered to the role of participant observer.

Phenomenological inquiry involves interviews as a key data collection strategy (Creswell, 2013; Moustakas, 1994; Patton, 2002). The current study included the use of face-to-face interviews requiring interaction with the participants. The participant observer role allowed me to interact with participants while using multiple senses to collect comprehensive data. In a face-to-face interview, the researcher can use sight to analyze the body language and facial expressions of the participants. Further, the researcher can use hearing to listen to the responses and notice distress or other emotion in the participant's tone of voice. Depending on the situation, researchers have the flexibility to adjust the role or degree of participation (Creswell, 2013).

Biases are "prejudice in favor of or against one thing" (New Oxford American Dictionary, n.d.). The background and experiences of a researcher can result in biases. The susceptibility of qualitative research to researcher bias acts as a limitation that can affect the objectivity of the study. In phenomenology, this limitation becomes stronger as researchers tend to be more connected to the research problem. The participants in this study were not related to me in any personal or professional way. The interaction with participants involved my role as a researcher with no power relationship over them.

Transcendental phenomenology encompasses a bracketing process that helps the researcher manage possible bias. Other strategies to manage bias include the use of an

interview protocol and semistructured questions. The interview protocol and semistructured questions facilitated focusing on the research problem and prevent deviation toward possible biases. The participant observer role enabled the use of probing questions and other strategies to stimulate and engage the participant. This level of flexibility aided the collection of comprehensive data about the cybersecurity phenomenon that otherwise may have been lost.

Methodology

Participant Selection Logic

The research design covers the population and "the unit of analysis to be studied" (Patton, 2002, Unit of Analysis, para. 3). The public sector constituted the finite population for this study. The lived experiences of public servants were the unit of analysis. The sample included public servants who had experienced the phenomenon while working in a municipal setting. IT leaders were defined as individuals performing senior-level IT functions.

Creswell (2013) recommended studying multiple sites as well as individuals. The San Juan – Carolina – Caguas MSA is the most populated area in Puerto Rico (U.S. Census Bureau, 2015a). The municipalities of San Juan, Bayamon, Carolina, Caguas, Guaynabo, Toa Baja, and Toa Alta have a population between 74,368 and 355,074 inhabitants. Table 1 shows the seven municipalities with their corresponding populations.

Criterion sampling takes into consideration cases meeting a "predetermined criterion of importance" (Patton, 2002, Criterion sampling, para. 1). For this study, the criteria included participants who were public servants; in IT leadership role; and had at

least 2 years of experience working within highly populated municipalities. The participants meeting these criteria had more experience with the phenomenon and were able to provide relevant data to the inquiry. A 2-step approach was followed to ensure that the participants met the criteria. The first step was working with municipalities listed in Table 1 to identify candidates who meet the criteria. A letter of cooperation was used with the municipalities to obtain their permission before reaching out to the candidates. The second step included corroborating the criteria with the participants. The criteria information of the participants was documented as part of the interview protocol.

Table 1

Populations of Research Sites

Municipality	Population
San Juan	355,074
Bayamon	189,159
Carolina	161,884
Caguas	134,481
Guaynabo	90,879
Toa Baja	82,065
Toa Alta	74,368

*Estimate from 2015 obtained from U.S. Census Bureau

Patton (2002) stated that "there are no rules for sampling in qualitative inquiry." Nevertheless, having an equal number of participants from each municipality may be a contributing factor to the credibility of the data. For consistency, the sample size was formed from an equal number consisting of two participants per site. A sample size of 10 to 14 participants can facilitate the collection of in-depth and reliable information.

Therefore, a minimum of 10 and a maximum of 14 participants were considered an acceptable sample size.

The process of identifying, contacting, and recruiting participants started after the approval of the Institutional Review Board (IRB). The first step was reaching out by phone to the municipalities listed in Table 1 to obtain their collaboration in the identification, recruitment, and interview locations. Their agreement to collaborate were documented in a letter of cooperation. The telephone conversation followed a script reviewed by the IRB which includes a summary of the purpose of the study, the sampling criteria, and verification that the public servants met the criteria. If the potential participants met the criteria, an invitation to participate was issued. If the potential participant accepted, a consent form with a sample of the interview questions, the explanation of the conditions for audio recording, and the confidentiality of participant information was sent by email to make official their participation in the study.

Creswell (2013) emphasized that the sample size is as important as the sampling strategy. Qualitative research provides a sense of balance between the breadth and depth of the investigation. This tradeoff provided the opportunity to concentrate on a smaller sample size to attempt to collect more data. In phenomenological studies, it is recommended to work with a sample size ranging from five to 25 participants (Creswell, 2013). A sample size within this range is sufficient to reach saturation. The study started with a minimum of 10 participants as an acceptable sample size. Depending on the level of saturation, up to four more participants could be recruited and interviewed for a total

of 14. This strategy ensured a positive relationship between saturation and sample size while providing the flexibility to concentrate on information-rich cases.

Instrumentation

A phenomenological approach was used to concentrate on the lived experiences of the participants. Therefore, the data collection instrument was crucial to capturing the essence the experiences of the participants with the phenomenon. Qualitative data consist of observation, interviews, documents, and audiovisual materials (Creswell, 2013). Each type of data can be subject to a variety of data collection techniques. Observing IT leaders performing during a cyber incident in person or through audiovisuals may not be appropriate due to potential legal concerns about exposing sensitive information. A similar situation could emerge in the review of artifacts that could be valuable to the study. However, artifacts such as security assessments, vulnerabilities, and security plans are exempted from public release under the FOIA of 1966. However, the use of interviews is appropriate for the proposed qualitative research plan.

Interviews served as the data collection instrument. Phenomenology "consists of in-depth and multiple interviews with participants" (Creswell, 2013, "Procedure for Conducting Phenomenological," para. 5). The intent of using this approach was to gain an understanding of how IT leaders perceive the cybersecurity posture of municipalities in Puerto Rico. Creswell (2013) and Patton (2002) agreed on the use of in-depth interviews with individuals who have experienced the phenomenon. Therefore, the methodology for the study included in-depth face-to-face interviews. The interviews incorporated open-ended questions and follow a semistructured protocol. Using a

semistructured protocol helped to maintain the participants within scope, and not limit their responses.

The protocol included a total of 13 questions. The questions were aligned with the research problem, the conceptual framework, and the literature review. This alignment in combination with the reviews of the Dissertation Supervisory Committee and the University Research Reviewer (URR) supported the content validity of the instrument. The interview protocol generated sufficient and relevant data. The themes and codes discovered during the literature review were associated with the dimensions influencing digital government and the questions in the instrument were related to these concepts. Appendix B includes the interview protocol with the 13 questions that were used as part of the data collection instrument. In addition to these questions, the interview protocol required the collection of information such as the date, place of the meeting, and confirmation that the participant is meeting the criteria.

Procedures for Recruitment, Participation, and Data Collection

The recruitment process consisted of contacting the selected municipalities to obtain their consent to recruit potential participants. Their collaboration in the recruitment process was part of a letter of cooperation established with each of the municipalities. Potential participants were contacted by phone to validate that they meet the criteria to participate in the study. If a potential participant expresses interest in the study or needs additional information before deciding to participate, a consent form was made available to complete the recruitment process. The purpose of the form was to provide a description of the research, details about the data collection, and to ensure voluntary

participation and confidentiality. The process continued until completing the recruitment of two participants per municipality for a minimum of 10. This sample size was aligned with Creswell's (2013) recommendation of using between five to 25 participants to achieve a deeper understanding of the phenomenon.

The data collection was performed via face-to-face interviews with the participants using an interview protocol. The interview was audio recorded. Patton (2002) explained that recorders do not remove the need for taking notes. Instead, recorders offer an opportunity to concentrate on taking strategic notes. For this reason, the plan included using a combination of field notes, mind maps, and audio recording. I was responsible for conducting the interview, taking notes, and setting up the recording. The combination of data types helped to prevent data overload by providing the means to go back to the audio, transcripts, or field notes to evaluate data that could have been overlooked during the collection process. The data collection event occurred once with each participant. The duration of the interviews was around 50 minutes.

If recruitment results in less than 10 participants or limited information for the study, the process could be repeated. If necessary, other municipalities within the San Juan – Carolina – Caguas MSA with a population higher than 70,000 such as Toa Baja and Toa Alta, could have been contacted. The participants entered and exited the interview after a debriefing that was part of the interview protocol. Follow-up procedures occurred by phone and e-mail to support the member checking strategy. Figure 4 shows all the highly populated municipalities that could have been targeted during the study.

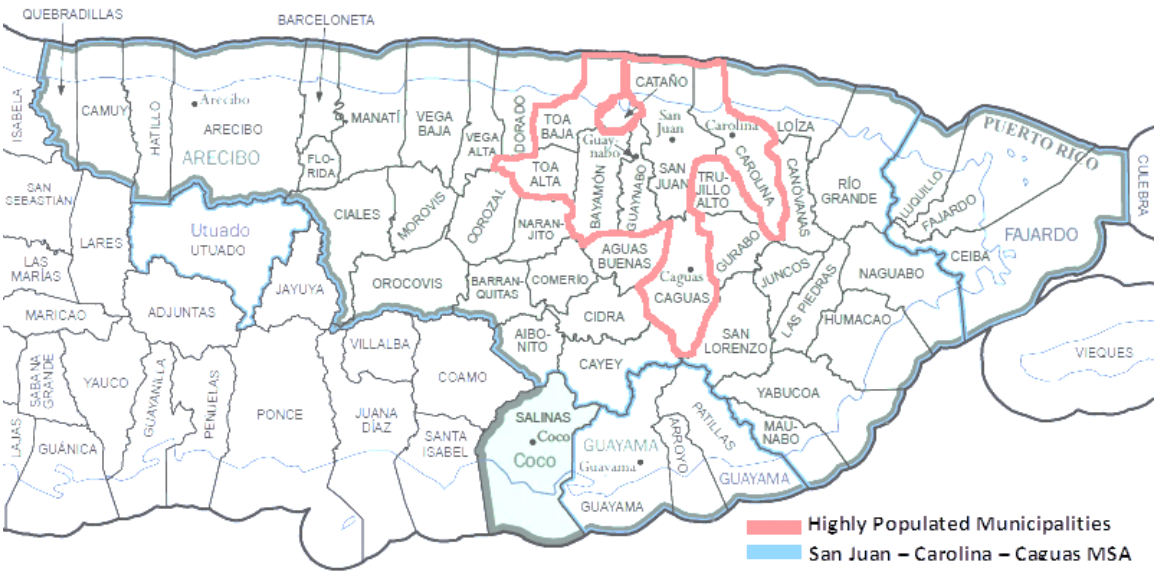

Figure 4. San Juan – Carolina – Caguas MSA and highly populated municipalities. Adapted from *"San Juan-Carolina, PR Combined Statistical Area"* by U.S. Census Bureau, 2012.

Data Analysis Plan

Organizing and coding the data from the field notes, mind maps, and audio recording were the initial steps in the data analysis process. These data types share an overlapping connection to the research questions. However, the mind mapping is related to RQ2. Mind mapping served as a "modeling technique which intends to portray ideas, beliefs, values, and attitudes and their relationship" (Burgess-Allen & Owen-Smith, 2010, p. 407). This technique facilitated the identification of the most influential factors for achieving a resilient cybersecurity posture and their relationship.

The field notes were planned to be captured using a computer and a word processor. The audio was recorded using a digital recorder. Later, the recordings were converted into transcripts. NVivo is a qualitative data analysis software used to support data coding, analysis, interpretation, and representation (QSR International, n.d.). After

organizing the data into a computer using files and folders, the data were uploaded into NVivo. The mind mapping was also transferred into NVivo. Horizontalization was the first step in the coding strategy. This process involved listing all the relevant experiences about cybersecurity expressed during the interviews. These experiences underwent a process of reduction, including grouping the horizons into "meaning units" (Creswell, 2013, "Phenomenological Analysis," para. 1). The initial meaning units started as codes that later were group into themes. The coding strategy utilized a combination of predetermined and emerging codes.

Creswell (2013) recommends starting the coding process with no more than six categories and then expand as necessary. The initial codes included elements such as policies, processes, collaboration, budget, and technology. NVivo's pattern-based automatic coding was attempted to facilitate the process. Then, codes were grouped into themes describing ideas related to the experiences of the IT leaders and the essence of the cybersecurity posture. These strategies contributed to describing the cybersecurity posture of the municipalities and in identifying those variables that according to the participants have the most significant influence on the phenomenon.

Clustering and thematizing were imperative for the interpretation and representation of the research data. Themes are defined as "broad units of information" (Creswell, 2013, "Describing, Classifying, and Interpreting," para. 6). These units are encompassed by invariant codes that when combined form an idea related to the theme. Creswell (2013) affirmed that selecting between five to seven themes is a common practice for data analysis. Emerging topics were discovered during the data analysis.

Burgess-Allen and Owen-Smith (2010) described mind maps as illustrations representing "concepts, ideas or tasks linked to and arranged radially around a central key word or idea" (p. 407). The primary branches departed from predetermined themes originating from the dimensions influencing digital government framework. The major ideas included concepts such as general, institutional, collaboration, organizational, data, and technology. The relevant experiences that cannot be clustered or labeled under the predetermined themes lead to the development of new themes.

After coding the data, a deeper analysis and interpretation was performed. The effectiveness of the data analysis techniques varies with the type of research approach. Creswell (2013) proposed a simplified variation of Moustakas' as the preferred data analysis technique to analyze data for a phenomenological study. First, the researcher's personal experience with the phenomenon was described through the process of bracketing. This process allows researchers to set aside personal experience and concentrate on the participants (Creswell, 2013).

Individual textural descriptions for each participant were developed as part of the process. These descriptions explained the state of affairs experienced by the participants (Creswell, 2013). Based on the textural descriptions, individual structural descriptions explaining how the experience occurred could be developed (Creswell, 2013). The analysis incorporated the textural descriptions into comprehensive passage known as a composite description. Creswell (2013) refers to this passage as the essence of the phenomenological experienced. Phenomenology studies "the common meaning for several individuals of their lived experiences of a concept or a phenomenon" (Creswell, 2013,

Definition and Background, para. 1). The composite description represented the experiences of the participants as a whole.

Discrepant cases were treated following the data analysis plan. During the horizontalization, all statements were given equal value. Then the cases were tested for reduction or elimination. This test included analyzing the relevance to understanding the phenomenon and fitting statements within the predetermined labels. If discrepant cases are relevant, but not aligned with codes and themes, new labels emerged as part of the clustering and thematizing process. Discrepant cases could provide a valuable alternate insight into the cybersecurity posture of government municipalities.

Issues of Trustworthiness

Credibility

Reviewing the data with the participants is essential for supporting credibility (Creswell, 2013). Member checking consists of sharing the "analysis, interpretations, and conclusion" (Creswell, 2013, Validation Strategies, para. 7) with the participants of the study. This strategy provided an opportunity to reach back to the participants for feedback on the researcher's interpretation versus the essence of their original statements. This strategy allowed the participants to provide an accurate judgment of the research data. The data were shared with the participants by email and was limited to the results.

External validity also plays a major role in the trustworthiness of the research. External audits can help to support the validity of the research. The Dissertation Supervisory Committee served as external auditors. The Committee included a content expert, methodology experts, and the URR. The content and methodology experts

provided guidance and support to ensure the quality and relevance of the research. These committee's members were engaged throughout all the phases of the research process. Similarly, the URR provided an additional layer of review which served as a quality assurance mechanism for the research. The committee's guidance and support were crucial to the quality and credibility of the study.

Transferability

Cybersecurity is a new phenomenon, in particular as it relates to the posture of the local government. Providing enough information to support the possible transferability of the study and the findings to other settings was crucial to help reduce the knowledge gap about this phenomenon. The literature review was presented in Chapter 2 with references to all the artifacts reviewed during the process. Chapter 3 provided a thick description of the methodology that could facilitate replicating the study in another setting. Any deviations to the design were discussed in Chapter 4. Furthermore, Chapter 4 included detailed descriptions of the settings, codes, themes, and other characteristics as a means for readers to determine the transferability of the findings to other settings.

Dependability

The dependability of the research was supported using audit trails, including artifacts documenting the identification of the problem, prospectus, literature review, research design, data collection instrument and evidence of the collection, data analysis, and interpretation of the findings. The identification of the research problem as well as preliminary frameworks, designs, methodologies, and implications were captured in a historical alignment tool. A prospectus outlining the problem, purpose, research

questions, and a high-level view of the proposed research design, framework and methodology were approved before starting the research.

The approved data collection instrument is available as in Appendix B. The data collection was evidenced by the interview schedule, field notes, and audio recording. These data types were used to support audit trails among the collected data. For instance, the audio recordings were converted into transcription to be compared with the field notes and mind maps. This strategy supported dependability by allowing me to cross reference the different data sources. Lastly, the interpretation of the findings was documented in composite descriptions that were validated through member checking.

Confirmability

According to Patton (2002), confirmability is essential to reducing bias, improving accuracy, and supporting impartiality of the research. The National Research Council (2009) states that the values that apply to research are the same values that relate to life. These values include "honesty, fairness, objectivity, openness, trustworthiness, and respect for others" (National Research Council, 2009, p. 3). Researcher bias can interfere with these values and the objectivity of the research which could lead to misleading results. O'Sullivan, Rassel, and Berner (2008) cautioned that researchers could influence qualitative research. The research design included bracketing as a form of reflexivity to support confirmability which was covered in Chapter 4.

Like dependability, confirmability is achieved through an auditing process (Creswell, 2013). Patton (2002) explained that auditing of the research process supports dependability. On the other hand, auditing the results supports confirmability. This

auditing process fell over “the doctoral committee for graduate students and peer reviewers for scholarly journals” (Patton, 2002, Expert Audit Review, para. 1). The Dissertation Supervisory Committee and the URR served as the auditors for the overall trustworthiness of the research. These strategies provided confirmability by clarifying research bias, suspending prejudgments, and maintaining objectivity.

Ethical Procedures

Identifying and addressing ethical concerns and risks are crucial in scholarly research, including human participants. Walden University (2015) offers a Research Ethics Planning Worksheet to assist in the identification and management of ethical concerns. This worksheet was used as the preliminary tool to identify and address ethical concerns throughout the proposed research process. After the research proposal was approved, the Application for Research Ethics Review was submitted to the IRB.

The IRB ensured that the research agrees with University’s ethical standards, as well as with pertinent laws and regulations to protect living persons from unethical practices and unnecessary risk as part of a research process (Walden University, 2018). The form included questions related to ethics, integrity, and confidentiality. The form required detailed procedures for recruitment and data collection, as well as for conducting a risk assessment. The form also covered conflict of interest, among other ethical matters. The supporting documentation approved by the IRB included the interview questions (See Appendix B), confidentiality agreement, and consent form. The IRB approval number was 11-07-17-0421741.

Treatment of human participants. The IRB application included a consent form as the artifact to gain access to the participants. After the approval of the IRB, this form was used to conclude the recruitment process by documenting the agreement of the participant to take part in the study. The consent form was distributed with enough time for participant review. This form included a description of the research, the data collection process, possible risk, and benefits. Further, the consent form explained that participation in the study is voluntary, and all information provided is kept confidential.

The treatment of human participants was performed with dignity and respect. The recruitment of participants was fair. As described in the sampling strategy, the subjects met the defined criteria. Studying the cybersecurity posture of local government as a social problem offered social value and scientific validity. The outcome of the research led to strategies that could help secure and improve government services while reducing cost and cyber threats against sensitive data and the availability of government systems. These benefits outweighed the risks and made of the study, worth participating.

Upon review, no ethical concerns were identified. The research design, data collection strategy, and data analysis plan were in line with the recommendations of Research Ethics Planning Worksheet. The recruitment method excluded special populations and vulnerable groups. An invitation to participate was sent to potential participants. If the participants were interested and met the criteria, the participants completed the consent form that was provided to take part in the study. Data were not collected without participant consent. Participants who refuse to participate could have been withdrawn from the study with no repercussion.

Before the interview, I reviewed the interview process, timeframe, and recording procedures to confirm the participants' understanding of the process and conditions. The interview commenced after making sure that the participants do not have questions and are in agreements with the terms of the interview. The member checking strategy supported quality by obtaining the reaffirmation of the participants. The interviews did not contain system-specific or vulnerability-specific questions to avoid endangering the participant's organization. These safeguards mitigated ethical concerns and ensured that the beneficence of this research outweighs the risks.

Treatment of data. Privacy and confidentiality are two important ethical concerns. I signed the confidentiality agreement assenting the responsibilities to safeguard the confidentiality of the participants and the data. Losing data can be detrimental to researchers and participants. If the information is lost, researchers may have to repeat the collection process. On the other hand, sensitive information can put the participants at risk. Creswell (2013) recommends masking the name of the participants to ensure confidentiality. The study did not collect sensitive information. Nevertheless, the data of the participants were stored using pseudonyms.

The research data were protected to ensure confidentiality, integrity, and availability. Miles, Huberman, and Saldana (2014) cautioned that researchers who do not take advantage of available technology would be disadvantaged in contrast with those who avail of available technology. Unfortunately, technology is subject to system failures and theft. Creswell (2013) recommends creating backups of the research data. Backups and cloud storage solutions are excellent strategies to ensure availability against data loss.

Google Drive was used as a cloud storage solution to help prevent data loss and allow access from anywhere in the world.

The data were stored on a personal computer and replicated into Google Drive. The computer was password protected, and the data were stored on an encrypted hard drive. The data replicated to Google Drive is secured using 2-step verification. This process requires a combination of username, password, and verification code (Google, n.d.). The verification code can only be received or generated by my phone. If the username and password are compromised, the attacker cannot access the information due to the missing verification code.

Raw data were not disseminated to any third party. Only the participants and I could access to raw data. During the member checking process, the results were shared with the respective participants for validation and feedback. The Dissertation Supervisory Committee could have access to the data to ensure the trustworthiness of the data collection, analysis, and interpretation after signing a confidentiality agreement. The final dissertation will be published in ProQuest upon receiving the approval of the University. I will attempt to disseminate the final research by publishing the investigation in scholarly journals. Since the research will not include sensitive information, the data will be kept for at least five years.

Summary

The research design provided the means to explore and understand the cybersecurity posture of municipalities in Puerto Rico. The design was based on the principles of phenomenology as a research tradition with a transcendental approach.

Transcendental phenomenology provided the scholarly structure for exploring, collecting, organizing, analyzing, and presenting information about cybersecurity postures during the research process. This phenomenological approach took advantage of researchers as the primary data collection tool.

I performed as a participant observer and did not have any relationship with the participants. The population consisted of public servants, while the sample consisted of public servants acting in IT leadership roles in municipal government within Puerto Rico. The study concentrated in highly populated municipalities within the San Juan – Carolina – Caguas MSA. It is expected that these municipalities had a more complex infrastructure and a higher dependency on IT systems. Part of the criterion was for the participants to have at least 2 years of experience with the phenomenon to guarantee an adequate level of experience and offer relevant data. Phenomenological studies could include up to 25 participants (Creswell, 2013). However, the larger the sample size, the shorter the depth of the research. The study consisted of a sample size of 10 participants to concentrate on gaining a deeper understanding of the phenomenon.

According to Creswell (2013), phenomenological studies rely mainly on interview data. Analyzing interviews from different participants could lead to the finding of shared or similar experiences that may be significant to address the research problem. This study used a researcher-developed data collection instrument consisting of in-depth face-to-face interviews following a semistructured protocol. This approach enabled participants to describe the essence of their experiences with cyber threats.

The data analysis plan leveraged the use of technological resources including NVivo, Google Drive, as well as other general software. NVivo served as the qualitative data analysis software for the organization, analysis, interpretation, and visualization of the data. Google Drive was used as the secure cloud solution for storing all the research data. The coding and them strategies consisted of a combination of predetermined and emerging elements. Predetermined codes emerged from the literature and the conceptual framework of the study. Emerging elements arose during the data analysis process.

The trustworthiness of the study was supported by validation strategies such as clarifying research bias, member checking, and external audits. Researcher biases were managed through bracketing. This process allowed me to provide an insight of my experiences with the phenomenon to support objectivity and the use of intuition which is fundamental to transcendental phenomenology. Member checking was used to share the results of the findings with each of the participants. Also, the Dissertation Supervisory Committee composed of a content expert, methodology experts, and URR served as the external auditor to the process and related process.

The ethical procedures included using a Research Ethics Planning Worksheet to identify and address possible ethical concerns. Further, an Application for Research Ethics Review was submitted to the IRB to ensured that the research met ethic requirements and aligned with the University's ethical standards and applicable ethical regulations. Participation in the study was voluntary and confidential. Participants were required to complete consent forms to participate in the research. Further, the research

data were safeguarded through the implementation of administrative, operational, and technical controls to preserve the confidentiality, integrity, and availability.

The next chapter included an overview of the outcome of the study. During Chapter 4, research elements such as the setting, data collection and analysis, evidence of trustworthiness, and results were described. Chapter 4 provided a thick description of the performed research methodology and its alignment to the research design described during this chapter. These descriptions supported the transferability of the findings by providing enough information for readers to determine if the results could be transferable to their knowledge settings. Also, deviations to the proposed methodology were explained and justified as part of the upcoming chapter.

Chapter 4: Results

The purpose of this study was to understand the cybersecurity posture of municipal governments from the perception of public servants serving in IT leadership roles in Puerto Rico. The principal factors affecting the cybersecurity posture of municipal governments were also addressed as part of the study. A phenomenological approach was used to address the knowledge gap about this problem. This approach focused on the lived experiences of IT leaders as information-rich cases.

Two qualitative research questions guided the study. These research questions addressed the perceptions of IT leaders' regarding the phenomenon of inquiry. The first research question addressed how public servants in IT leadership roles perceived the cybersecurity posture of local government municipalities in Puerto Rico. The second question addressed the factors that public servants in IT leadership roles perceived to be most influential in achieving a resilient cybersecurity posture.

The research methodology did not include a pilot study. Also, demographic data were not collected to safeguard the confidentiality of the participants. The sections of this chapter include the results of the study related to the purpose and research questions. This chapter also covers other related research elements such as the setting, data collection, data analysis, and trustworthiness of the data. This chapter offers a thick description of these research elements. Further, deviations from the original methodology are explained and justified.

Research Setting

The research setting encompassed highly populated municipalities within the San Juan – Carolina – Caguas MSA. This organizational condition of highly populated municipalities required managing budgets, services, and information resources in alignment with the size of the population. These conditions had a positive influence on the participants to support their development as information-rich cases. Other conditions that could have influenced the experiences of the participants with cybersecurity participants were political changes, fiscal situation, and natural disasters.

After the 2016 election in Puerto Rico, the political leadership administering the targeted municipalities remained unchanged. However, in June of 2017, the mayor of Guaynabo resigned from his position (Suarez-Torres, 2017). After a new election, a new mayor from the same political party was elected having minimum impact on the participants. This condition provided continuity of operation for the participants performing in IT leadership roles within the municipalities.

The fiscal crisis also affected the participants and their organizations. Since January 2017, the oversight board established by the Puerto Rico Oversight, Management, and Economic Stability Act (PROMESA) of 2016 was responsible for approving fiscal plans and budgets as well as requesting their revision and enforcing requirements upon them. The government budget had been reduced, directly affecting the targeted municipalities and their IT operations.

Another significant factor affecting the participants and their experiences was the aftermath of hurricane Maria. In September 2017, a Category 5 hurricane devastated

Puerto Rico leaving its critical infrastructures such as the telecommunications, power grid, and water and wastewater systems inoperable. Most of the municipalities that participated in this study spent an average of 3 months without electricity. This situation increased the participants' experience in disaster recovery efforts supporting the availability of their systems. The situation also limited the availability of the participants in these municipalities. Participants in the municipalities of Toa Baja and Toa Alta were planned to be part of the study, but they could not be reached due to the lack of electrical power and problems with telecommunications after hurricane Maria.

Data Collection

The data collection process started on May 7 and lasted until May 18 of 2018. During the recruitment process, 10 public servants working in an IT leadership role in a municipal setting in Puerto Rico were invited to participate in the study. A total of 10 public servants agreed to participate in the study. The municipalities that took part in the data collection were San Juan, Bayamon, Carolina, Caguas, and Guaynabo. A combination of field notes and audio recordings was used to collect the data. The data collection process was performed during face-to-face interviews with the participants.

The interviews took place at the participants' place of work. Seven of the participants were interviewed in private offices. Three participants were interviewed in conference rooms. Both the offices and the conference rooms offered security and privacy to the participants. The frequency of the interviews was limited to one session. The duration of the sessions lasted an average of 1 hour. Before the interviews, 10-minute briefings were performed to describe the study and the conditions. After the initial

briefing, the session advanced to the interviews, which lasted an average of 45 minutes. Each interview was followed by a 10-minute debrief to answer any questions from the participant and to explain the next steps in the process.

During the interviews, I wrote field notes in a notepad. With the consent of the participants, the interviews were recorded. The primary method for the audio recording was a smartphone application named Audio Recorder, which was developed by Sony under the Android Open Source Project. A second recording device was used as a backup to the smartphone application. The secondary device was a Yemenren 8GB Sound Audio Recorder Dictaphone.

Three minor deviations transpired from the data collection plan presented in Chapter 3. The first deviation was capturing the field notes in a notepad instead of in a digital format using a computer. The notepad was less distracting and helped to foster a better interpersonal connection with the participant. The second deviation was drafting mind maps during the interviews. Mind maps were not used during data collection because the process reduced emphasis on from the interview. Instead, the emphasis was placed on the field notes, which were crucial to developing probing questions using the participant's examples. The third deviation was two of the eight interviews were not one-on-one. Due to lack of time and conflicting priorities, one interview was scheduled with two participants at the same time. The person in the primary leadership role served as the primary participant and the second person performed a supporting role to provide additional information.

Data Analysis

After collecting the data, I used a text-based toolkit product named Trint to transcribe the audio recording. I reviewed the transcripts for quality and mechanics. Then, I translated the transcripts from Spanish to English and entered into NVivo. Two deviations from the original data analysis plan occurred. The first deviation was not using NVivo's pattern-based automatic coding because this capability was in an experimental stage and could have affected the trustworthiness of the study. The second deviation was the use of structural description. This description requires deep insight from the participants that could lead to their identification, and the study was designed to keep the identity of the participants confidential. Beyond these deviations, the data analysis was performed according to the plan. The data analysis followed a phenomenological approach consisting of horizontalization, reduction and elimination, clustering and thematizing, validation, and individual and composite textural descriptions. Each phase was recorded in NVivo as shown in Figure 5.

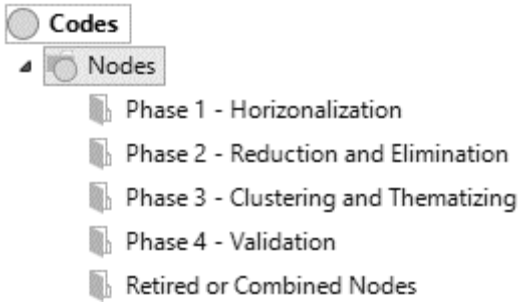

Figure 5. Data analysis phases documented in NVivo. This figure illustrates the phenomenological data analysis phases as documented in NVivo qualitative data analysis software.

During the horizontalization phase, all of the relevant experiences about cybersecurity expressed during the interview were identified. The experiences were given

equal importance. I noticed a connection between the participants' experience and the security controls listed by NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, particularly regarding the controls required for low impact systems. A total of 106 items emerged as part of the initial coding process.

The second phase consisted of reduction and elimination. The 106 codes were reviewed to validate that the experience was necessary for the understanding of the phenomena. During the reduction process, the initial codes were grouped into meaning units (see Creswell, 2013). The second step was the process of elimination. During this process, the codes were reviewed taking into consideration possible overlaps, repetition, and vagueness. Through the processes of reduction and elimination, the codes were reduced to 58 codes, almost half of the initial coding.

The next phase of the data analysis was clustering and thematization. During this phase, meaning units were clustered into broad units of information or themes (see Creswell, 2013). As explained in Chapter 3, the codes included a combination of predetermined and emerging codes describing ideas related to the experiences of the IT leaders and the essence of the cybersecurity posture. The codes were analyzed to align with Creswell's (2013) recommendation of five to seven themes. The first six themes were aligned with RQ2 and the dimensions of the conceptual framework. These codes included general, institutional, collaboration, organizational, data, and technology dimensions. The seventh code emerged later in the process and was aligned with RQ1 and was labeled as posture. Another theme was created to capture administrative data such as memorable quotes. All of the emerging themes were within the scope of the

conceptual framework's dimensions and were clustered as subthemes under the applicable domain. With the additions, the codes increased from 58 to 66.

The fourth phase was validating the codes and themes. I followed three steps recommended by Moustakas (1994):

- Are codes and themes expressed explicitly in the complete transcription?
- Are codes and themes compatible if not explicitly expressed?
- Delete not explicit or compatible codes and themes.

Based on the guidance from Moustakas (1994), I removed not explicit codes and themes. The codes that were identified as not compatible but valid to the study were moved to compatible nodes. Those identified as not compatible with the study were deleted. During the validation phase, the themes were aligned with the cybersecurity-related areas listed in Federal Information Processing Standards (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems, rather than individual security controls. Table 2 shows an overview of FIPS 200 cybersecurity-related areas referenced by the participants as information-rich cases. After the validation phase, the total nodes were narrowed to 46.

The next step in the process was the development of individual textural descriptions. Using NVivo, I aligned the initial data file containing the interview transcripts with the coding of meaning and broad units of information as the foundation for the textural descriptions. These textural descriptions were incorporated into comprehensive passages known as a composite description representing the experience of

the participants as a whole. The composite description was used as the content for the study results. My interpretation of the composite description is presented in Chapter 5.

Table 2

Minimum Cybersecurity Requirements Areas Referenced by Participants

Cybersecurity-Related Areas	Referenced	Cybersecurity-Related Areas	Referenced
Access Control	Yes	Media Protection	No
Awareness and Training	Yes	Physical and Environmental Protection	Yes
Audit and Accountability	No	Planning	No
Certification, Accreditation, and Security Assessments	No	Personnel Security	No
Configuration Management	Yes	Risk Assessment	Yes
Contingency Planning	Yes	System and Services Acquisition	Yes
Identification and Authentication	No	System and Communications Protection	Yes
Incident Response	Yes	System and Information Integrity	Yes
Maintenance	No		

Note. Cybersecurity-related areas were adapted from the Federal Information Processing Standards (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems.

Discrepant cases were managed as part of reduction and elimination, clustering and thematizing, and validation. The cases were tested during the reduction and elimination to validate relevance and labeling. The discrepant cases that were relevant but not aligned to existing codes emerged as new labels. A similar approach was followed during the clustering and thematizing phases. During the validation phase, all of the nodes were validated following Moustakas's (1994) validation strategy.

Evidence of Trustworthiness

Credibility

The documents used to support the research were peered reviewed or originated from reliable sources such as government agencies. The participants were public servants in IT leadership roles who had experienced the phenomenon. A member checking technique was used to support credibility and validate the analysis, interpretations, and conclusions. A summary of the results with the key themes was emailed to the participants. The intent was for the participants to provide reassurance of the results and identify possible gaps or misconceptions. The participants did not report discrepancies with the results. The deviations to the strategies presented in Chapter 3 were explained and justified as part of the Data Collection and Data Analysis sections.

Transferability

The literature review was presented in Chapter 2 with references to all of the artifacts reviewed during the process. Chapter 3 provided a thick description of the methodology to facilitate the replication the study in another setting. This chapter provided a thick description of the settings, codes, themes, and other characteristics as a means for readers to determine the transferability of the findings to other settings. The deviations were discussed in the Data Collection and Data Analysis sections and should have no significant impact on the transferability of the study.

Dependability

The dependability of the research is supported through audit trails, including artifacts documenting the identification of the problem, prospectus, literature review,

research design, data collection instrument and evidence of the collection, data analysis, and interpretation of the findings. The identification of the research problem as well as preliminary frameworks, designs, and methodologies were captured in a historical alignment tool. A prospectus outlining the problem, purpose, research questions, and an overview of the research design, framework and methodology were approved before starting the research. The approved data collection instrument is in Appendix B. The data collection audit trail includes audio files, transcript, and translated transcript that are stored as data files in an NVivo project. This strategy supports dependability by allowing cross-referencing the different data sources used in the research.

Confirmability

The research design included bracketing as a form of reflexivity to avoid biases. In addition to bracketing, Creswell (2013) mentioned that auditing could be used to support confirmability. Similar to the approached described in the Dependability section, each phase of the data analysis is documented in individual folders inside the Codes sections of the NVivo project, including a folder for retired and combined nodes as documented in Figure 5. The folders are linked to memos with insight on the process. The individual and composite textural descriptions are documented in memos within NVivo. Also, the mind map and visual representation of the results were developed using NVivo. The Dissertation Supervisory Committee and the URR served as the auditors for the overall trustworthiness of the research. These strategies provided confirmability by clarifying research bias, suspending prejudgments, and maintaining objectivity.

Bracketing

I have 17 years of experience with cybersecurity at the federal government level while performing in different roles ranging from a system administrator to the information system security manager. Between 2014 and 2016, I was responsible for the cybersecurity of a national system that interconnected with 46 state-level systems. During this time, I was exposed to the posture of various states and local governments. Their posture was not mature which led to several collaboration initiatives to raise awareness and help improve their posture. The initiates included webinar and conferences as well as establishing minimum security controls, assessment of the controls, as well as developing federal regulation to mandate the use of information security agreements. These experiences could have contributed to biases against the posture of the local government. The Data Collection, Data Analysis, and Evidence of Trustworthiness sections on this chapter included some of the mechanisms used to counteract possible biases. Outside the research design, my personal experience during the research was contrary to any bias as it driven by curiosity and interest in participants' perception of the phenomenon.

Study Results

The results were organized in the predetermined and emerging codes discovered during the data analyses process. The results include quotes from transcripts and data visualization such as mind maps and hierarchy charts developed in NVivo to illustrate the results. The results start with a section titled Posture which answered RQ1. The remaining sections are associated with RQ2. Figure 6 shows a summary of the primary elements affecting the local government’s cybersecurity posture discovered in the study.

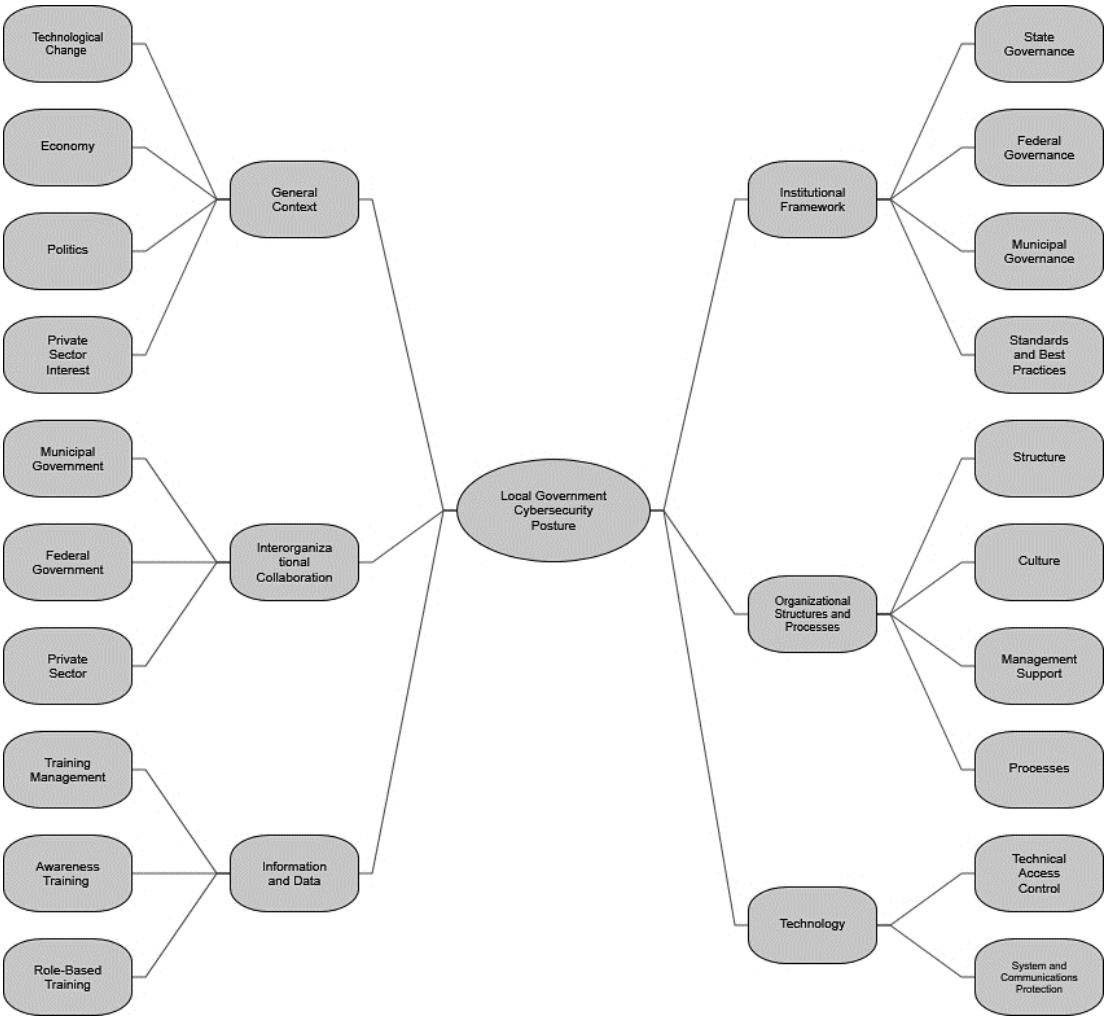

Figure 6. Mind map of dimensions and elements influencing digital government. This figure illustrates the dimensions that were part of the contextual framework of the research methodology in alignment with the elements identified as part of the results of the study as influential factors to the local government cybersecurity posture.

Posture

The participants perceived the posture of their municipality as resilient. P-3 stated, "on a scale of 1 to 5; I would say that we are a 4." Meanwhile, P-4 used the results from the comptroller's IT audit as a resiliency measurement where the municipalities with a low score "should not be very protected and that possibly they do not have the tools or processes to work with cybersecurity." The participants agreed that their

municipalities are more secure because of their ability to implement mature processes. Figure 7 shows the Organizational Structure and Processes as the most relevant dimension supporting the posture of the municipal government.

Outside their municipalities, the participants talked about the posture of federal and state government as an influential factor to their own. These postures were captured as part of the Institutional Framework as identified in Figure 7. However, most of the data were about how this dimension is failing to provide the conditions to support cybersecurity. P-3 described the federal government as stringent while the state was seemed as flexible with cybersecurity. P-8 revealed using stricter processes to protect health data due to federal requirements. P-3 said that insularism prevents the state from seeing "what happens in the world of cyberattacks and we are alienated from our political relationship with the United States where things that affect them will eventually affect us." P-6 said that most incidents happened at the state and summarized the overall posture as "some agencies give more love to cybersecurity than others."

The participants identified the information and technology dimensions as critical supporting elements. P-2 expressed feeling "safe with the technologies that we have in place." P-3 pointed to technology as the reason they can provide the same services as other municipalities, but with more accessibility, efficiency, and security while recognizing that technology alone does not make them invulnerable. P-7 considered technologies and processes among other elements, to be of equal value stating, "I understand that all the factors are equally important because if you implement one thing without implementing the other, you will not reach a resilient posture." P-1 mentioned,

"there is always room for improvement" and is confident that "little by little" the posture can be improved. The rest of the participants also acknowledged having areas to improve.

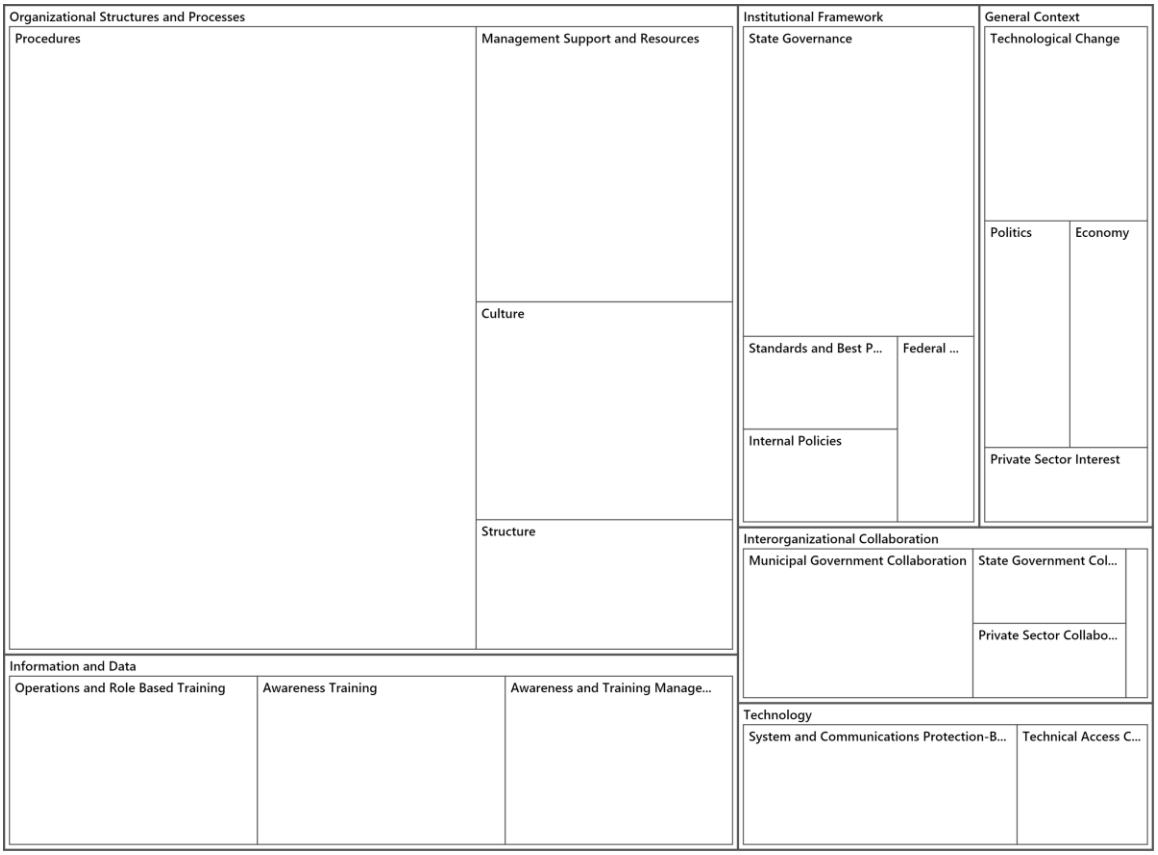

Figure 7. Hierarchy chart of dimensions and elements supporting cybersecurity. This figure provides a hierarchical view of the dimension and element, and their influence on the local government cybersecurity posture. The bigger the area, the more relevant to the posture.

General Context

The general context dimension encompassed the external factors affecting the cybersecurity posture of the municipalities. These factors were identified by the participants as changes in technology, economic situation, political agendas, and the interest of the private sector.

Technological change. As seen in Figure 7, the participants identified technological change as the general context element with the most significant impact on their posture as it encompasses multiple threats and challenges. P-3 explained that IT services have evolved from one office with a system and dedicated administrator into multiple systems, networks, and teams devoted to supporting a vast range of IT services. P-1 explained:

> The Internet has been around for many years, but the access to it has increased, and with higher bandwidth and increased in services there is more exposure. That transition led the municipality to provide online services, but there is no education about the risks.

P-1, P-3, P-4, P-5, and P-7 agreed that cybersecurity is an ever-changing domain. P-5 stated, "policies change, security changes, viruses, and attacks change." P-4 recognized that business processes are mobility and data-driven and recommended adopting cloud technologies to address some of the challenges. However, P-7 warned about the risks and exposure of cloud service providers to frequent attacks and explained that attackers prefer targets that will give them more data and reputation versus a municipality.

P-5 explained that instead of technical knowledge attackers are relying on scripts, tools, and the Internet to execute attacks. P-1 stated, "organizations believe that they will not be victims of cyberattacks because their data are not of interest." P-5 warned about attacks designed to lure users through phishing emails, website spoofing, and rogue

wireless hotspots. P-1 affirmed that attacks like ransomware "encrypt social security and credit card information in the same way that will encrypt nonconfidential information."

P-7 stated, "you block one thing, and half an hour later you are being attacked by other means because hackers are always looking for ways to do damage." P-6 said, "I can buy a great appliance, but there is already a hacker trying to compromise the system." P-8 agreed and stated, "if you stay behind it will be much easier for someone to attack you." P-4 stated, "a lot of people out there trying to enter and get information. Therefore, what worries me the most is not knowing what is happening?" P-4 cited Murphy's Law and advised being vigilant even when nothing seems to be happening.

Economy. P-1, P-3, P-4, P-5, P-6, and P-7 highlighted the fiscal situation as an element affecting the availability of resources. P-6 stated:

> The municipalities of Puerto Rico economically are not well. Before the hurricane, I went to another municipality where for economic reasons employees only worked half-days. If they do not have a budget and their employees work half-days, they will not have money to purchase cybersecurity equipment.

P-3 identified PROMESA as one of the factors affecting the government's budget. The situation has also affected the staff as P-6 said, "some employees are very committed and others who are disgruntled because they have not had salary increases, bonuses were eliminated, and sick days were reduced." P-3 believes that the government should not "use money as an excuse to do not do the things that must be done. We must do things well, ethically, morally, and legally regardless of whether there is money or not."

Politics. P-3 mentioned that diverse political ideologies could turn into fanaticism affecting operations and services. P-7 considered that having 78 municipalities nourish division and repetition. Several participants agreed and endorsed consolidation strategies. Each municipality has a data center to what P-6 asked: "Why do we need so many data centers providing the same services?" P-6 uses the private sector as an example of data center consolidation to reduce cost and identified politics as the main obstacle. However, P-6 stated, "If I try to consolidate using my data center, the municipalities of the opposite political party will not agree." P-5 mentioned that politics has also affected interoperability and explained that during hurricane Maria, the government was using different frequencies instead of a standard emergency channel.

Private sector interest. P-5 mentioned that private sector interest leads to recommending products that are not the best for the municipality with the intention of making a profit or taking out the competitor. According to P-5, these interests expand to the telecommunication services where private entities after buying other companies had broken preestablished agreements preventing the reuse of relay towers by other providers resulting in a degraded infrastructure. P-5 and P-8 revealed that providers are not diligent with resolving outages, often taking days to fix them. P-8 described the telecommunication market as a monopoly.

Institutional Framework

The participants gave a similar value to federal governance, standard, and internal policies as evidenced in Figure 7. These elements were identified as important, but not as current influential factors. For instance, P-8 indicated complying with the Health

Insurance Portability and Accountability Act of 1996. On the other hand, most participants expressed a lack of familiarity with federal policies and international standards such as those developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). P-4 mentioned that federal guidelines are useful and more accessible than the ones provided by the state. P-5 recognized the importance of following these guidelines but explained that the municipalities only follow the comptroller's guidance which does not include federal or international requirements. According to P-6, not having a federal point of contact is a challenge to the voluntary adoption of federal guidelines. Regarding internal policies, P-3 revealed that the municipality has just an ordinance that regulates the use of information systems. P-5 recommended developing and implementing municipal policies that are more detailed than the state governance.

The municipalities are subject to the E-Government Act of 2004, TIGs, and circulars. P-3, P-6, and P-5 agreed that the state has failed to enforce compliance with the policies. P-5 stated, "If you have a law and you do not explain its use and not enforce it the law is just written on paper." P-4 and P-6 mentioned that the comptroller performs IT audits, but these are done infrequently. Also, P-5 and P-7 explained that the audits have no clear scope, plans, nor metrics. P-1 mentioned that often people learn of the requirements after an incident has occurred. P-5 and P-7 provided examples of findings from undefined requirements and explained that could have been addressed earlier if the requirements were clearly defined. P-5 acknowledged that ignorance is not an exemption, but points to lack of training and communication as the problem.

P-5 and P-8 agreed that policies must be established by the state without political interest while leveraging standards and ensuring enforcement. P-8 recommended making the circulars mandatory and explained, “improving legislation will force entities to follow an operational standard.” P-2 described the policies as “quite complete.” However, the rest of the participants contended that the policies are general and up for interpretation. The participants affirmed that the circulars are not practical nor readily accessible, the format requires analysis to understand changes and applicability, and without proper communication, the requirements can be lost. P-7 recommended establishing a living policy that is accessible and updated as new requirements are enacted.

In addition to the comptroller, the government established the CIO of Puerto Rico. P-6 and P-7 mentioned that the CIO is supposed to be watching over the entire government instead of just focusing on state agencies. P-7 affirmed that the CIO should be responsible for reaching out to the municipalities to understand the factors affecting their cybersecurity posture, develop solutions, and foster collaboration and information sharing. P-6 and P-7 identified information sharing as an area needing improvement, citing examples of state agencies that have been hacked. P-7 stated, “If we continue with the same concept of 78 municipalities and numerous government agencies where each one is doing something different, there are knowledge and experiences that are being lost.” The lessons learned are crucial to prevent future attacks. P-8 revealed that the state is legislating to empower the CIO to implement requirements across the government.

Interorganizational Collaboration and Networks

According to P-6, “collaboration does not exist much in Puerto Rico.” Similarly, P-7 expressed, “the culture of collaboration does not exist.” Figure 7 shows interorganizational collaboration as the second lowest relevant dimension. The participants mentioned that collaboration with the federal and state government was limited to emergency response or other compulsory conditions. P-1 and P-2 experienced collaboration as part of system interconnection efforts. P-2 stated, “It sounds nice, like we can work together, but is a matter of cybersecurity defense rather than genuine collaboration.” Nevertheless, most of the participants recognized the lack of collaboration as a negative factor and expressed their wiliness to collaborate.

P-3, P-4, and P-7 identified emergencies as collaboration opportunities. P-7 revealed that most municipalities “do not have the budget to have a disaster recovery center, and after the hurricane, their fiscal situation is worse.” P-7 recommended establishing agreements to receive essential IT services from the municipalities proven to withstand a hurricane. Also, P-3 shared being part of a coalition of municipalities and stated, “the economic resources needed to maintain cybersecurity are too high, and in this coalition, we help each other.” Regarding the private sector, collaboration was limited to service contracts. P-4 planned to benchmark processes and technologies with public and private entities and affirmed that these enhancements could not be achieved in isolation.

Organizational Structures and Processes

Contrary to the general context dimension the organizational structures and processes encompassed the internal elements of the organization. These elements are

related to the organization's ability to defend and protect against cyber threats. As shown in Figure 7, the organizational structure and processes dimension was identified as the most influential dimension to support resilient cybersecurity posture.

Structure. The participants identified centralization as the most effective structure to manage cybersecurity but agreed that the structure should be tied to the size, type, resources, and complexity of the organization. From a technical view, P-5 and P-8 justified centralization to secure and monitor the network and communication routes. P-2 stated, "every agency should have one person in charge of cybersecurity." However, P-1 and P-7 affirmed that most agencies do not have a dedicated role. P-3 and P-5 explained that the IT office is divided into areas with cybersecurity as an additional function. P-7 stated, "this role is assigned to someone who already has another pile of things to do. Therefore, you do not have a person with a clear mind to focus on this topic." P-1 identified the network engineer as the person usually performing this role.

Culture. P-1 stated, "cybersecurity is taken very lightly, I do not think it is looked with the attention it deserves." P-1 shared working at organizations where "cybersecurity is done to check the block and say that there is something in place." P-7 affirmed that the concept of cybersecurity is new and is not part of the culture. P-2 mentioned, "people are resistant to change, especially when is related to technology." P-5 explained that users still writing their passwords and keeping them under the keyboard and does not give credit to IT staff unless a system is down. P-4 agreed and described cybersecurity professionals as silent heroes working to prevent incidents. However, cybersecurity professionals are seen as bad guys for restricting access. P-4 stated:

> I am one of the least popular people because one of the first things I did was implementing password controls such as password expiration and complexity. I still am a persona non grata because later I reduced access to the Internet and social media.

Management support and resources. Figure 7 identified management support as one of the most relevant elements in the study. Participants agreed that management's commitment is an influential factor, because managers are responsible for assigning resources. P-3, P-4, P-6, and P-8 shared having a good experience with management. P-6 described management as “pro-technology” and “very tech-savvy.” P-4 stated:

> Management support has been good at supporting cybersecurity. Whenever we have asked for a budget, management has seen the importance and are aware of the need for investment. That is why we have been able to maintain good programs and resources.

However, P-3 described as difficult explaining to management why a system that is functional is no longer supported and must be replaced. P-1 explained, “cybersecurity is not seen as something that will bring a return on Investment (ROI), especially when in the last 10 years nothing has happened” P-3 and P-5 recommended presenting cost reductions, service improvement, operational enhancements, and tradeoff as ROI. P-3 pointed at virtualization as an alternative to reduce cost by turning old computers into thin clients. P-2 recommended, “projects that can be subdivided into blocks that can be carried out over several years.” P-7 stated, “to have the best employees you cannot offer

the worst salaries" and shared an initiative that has saved around 20 million dollars in the last 10 years by hiring staff with the proper skills and compensation.

Processes. Participants shared a vast experience of organizational processes. As evidenced in Figure 7, processes were identified as the most relevant element supporting the cybersecurity. Figure 8 provides a closer look at the list of procedures that were identified by the participants as key to support their cybersecurity posture.

Access control. Processes like account management made of access control the third most relevant procedure and one of the most significant elements of the organizational structure and process dimension. P-2, P-3, P-4, P-7, and P-8 shared similar account management procedures where new staff agrees to the system use policy, and a copy of the agreement is kept in a file. P-5 uses system use notification banners to remind users of the conditions in the use policy. For calls related to password, P-5 requires identity verification consisting of security questions, supervisor validation, or a valid identification. P-5 and P-8 mentioned disabling the accounts of users on extended leave or those no longer with the agency. Most participants confirmed using role-based controls to configure access based on the user's responsibilities. P-8 says the goal is to make it hard for a disgruntled employee and external attackers to be successful. P-5 and P-8 mentioned that only administrators have privileged access to the systems. P-4 and P-5 identified separation of duties as a deficiency explaining that some administrators have the same access because of the need to be each other's alternate to ensure coverage.

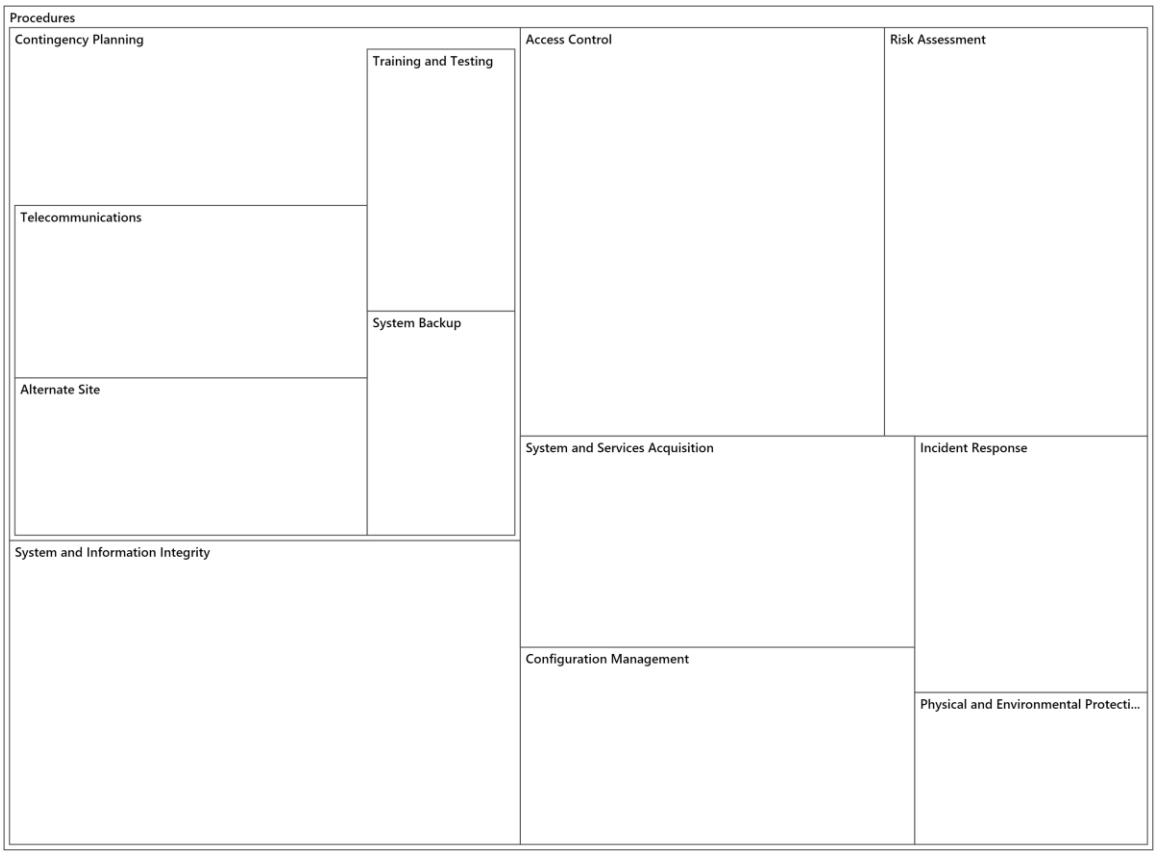

Figure 8. Hierarchy chart of processes supporting cybersecurity. This figure provides a hierarchical view of the key process and subprocess, and their influence on the readiness of the organizational structures and processes dimension. The bigger the area, the more relevant to the posture.

Configuration management. P-2, P-5, and P-8 perform configuration management over open ports/protocols/services to ensure that these are closed by default and allowed by exception. P-1 recommended introducing cybersecurity at the beginning of the system development lifecycle by including minimum requirements such as secure protocols, encryption, and network segmentation. P-4 emphasized the proper configuration of security tools to take advantage of all of their protection capabilities. P-5, P-6, and P-7 mentioned that removable media ports are blocked by default and allowed through an approval process. P-3 and P-7 are proponents of the thin clients configured

with least functionality. P-5 mentioned using media access control address filtering to control access to the wireless network.

Contingency planning. The frequent exposure to hurricanes and the recent experience with hurricane Maria made of contingency planning the most relevant process. P-1 described the experience with hurricane Maria as "frightening" and identified contingency planning as the number one priority. Figure 8 describes the relevance of contingency planning and its related elements in comparison with the other processes. P-8 explained, "when hurricane Maria struck, Puerto Rico was without electricity and other services, but the municipality was operational." The contingency plans were key to the success of their continuity of operations. Figure 9 shows a mind map of the processes and contingency planning subcomponents identified in the study.

Contingency training and testing. P-4, P-5, P-7, and P-8 advised testing and reviewing contingency plans as well as related sites and systems. P-7 acknowledged that the contingency efforts failed and incorporated testing to avoid future incidents. P-5 shared a situation in which change was made, but not replicated on the alternate site, and the monitoring tools did not identify the discrepancy. However, during a testing exercise, the situation was discovered and corrected. P-5 also recommended stress testing stating, "if you do not do the simulation, you will not know if the system will be available." P-5 affirmed that testing for availability is as necessary as any other test.

Alternate sites. P-3 affirmed not having "all the eggs in one basket" as their strategy included alternate site, redundant data, and voice with different providers. The participants shared having alternate storage and processing sites as well as performing

data replication. P-4 uses a hybrid cloud colocation, P-6's alternate site includes a workspace, and P-8 mentioned having two data centers with mirrored equipment to serve as each other alternate. P-3 mentioned that virtualization help contingency efforts as systems could be deployed and accessed from anyplace with Internet access.

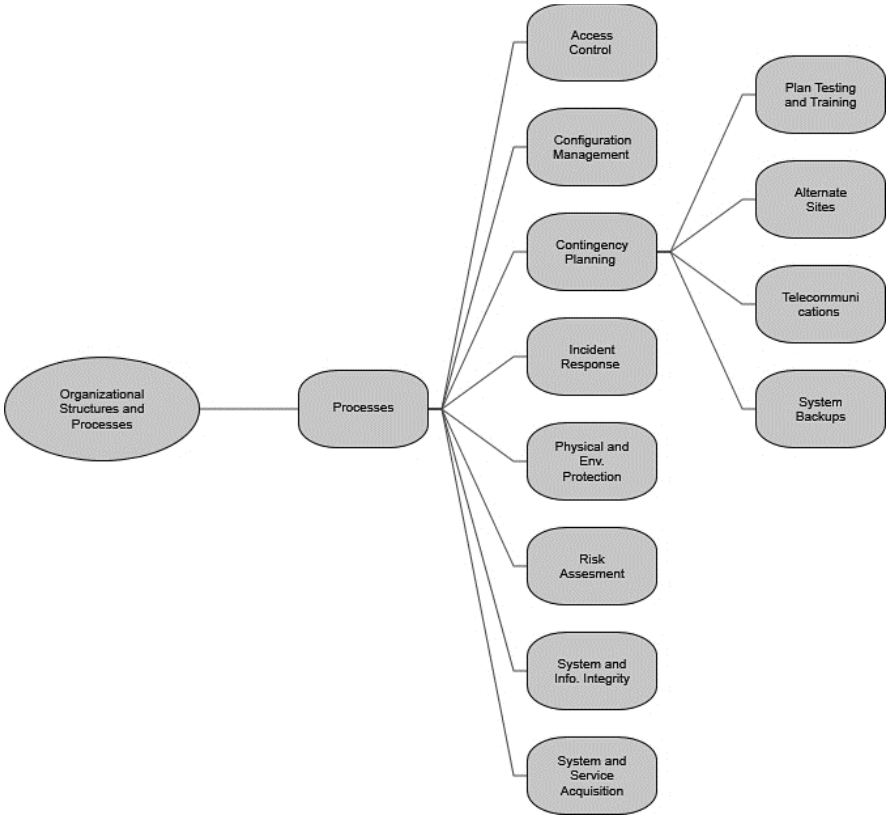

Figure 9. Mind map of key processes supporting cybersecurity. This figure illustrates the key processes and subprocess supporting the cybersecurity posture of the local government and their relationship.

Telecommunications services. P-4 discovered the difference between critical assets during normal operations and a time of crisis and identified telecommunications as the most critical assets. P-5 explained, "if the telecommunications go down, not only did you lose the data, you also lost your voice and you were left without communications

unless you have redundancy." P-3, P-4, P-5, and P-6 mentioned having redundant network connections using fiber optic and wireless with different providers.

System backups. P-7 stated, "is very important to have good backups because it is the only thing that can guarantee that you can return your systems to a given point in time in case of an attack or natural disaster." Most participants mentioned their system backup strategy includes backing up critical systems more often in addition to scheduling tape rotation between internal and external archives.

Incident response. P-3, P-4, and P-7 revealed being affected by ransomware. P-4 explained that while recovering from a blackout "someone notified us that he could not access his data, but we understood that it was part of the recovery process, but it was ransomware." The root-cause analysis pointed to a computer used for constituents to upload documents. As part of the lessons learned, P-4 established controls to prevent executables files while allowing formats required for the services. P-3 and P-4 were able to recover using their backups. In the case of P-7, the incident happened at a thin client, and instead of paying the ransom P-7's team restored the system to the previous day.

Physical and environmental protection. According to P-4, cloud service providers have everything necessary to operate out of the grid for months. Outsourcing those services prevented investing in the systems to support those conditions. P-5's alternate site can operate for 30 days disconnected from the grid. The site consists of redundant water tanks, power generators, heating, ventilation, and air conditioning, and uninterruptible power source batteries. P-8 also shared having redundant power

generators and batteries. P-5 mentioned using security cameras, closed cabinets, access cards, in addition to access logs, and limited physical access to key personnel.

Risk assessment. P-4 mentioned that data must be protected based on their risk and identified financial and PII data as the priority. P-4 explained that public information also needs to be protected to avoid its release outside established protocols. P-3, P-5, and P-7 expressed that often the personnel responsible for cybersecurity are not experts, and outsourcing external assessments such as penetration testing are crucial to validate the security controls. P-5 and P-8 recommended performing risk assessments at least twice a year. P-7 mentioned that the comptroller requires external assessments, but the fiscal situation is an obstacle to justifying the cost.

System and information integrity. The participants acknowledged using a centralized approach to managed malicious code protection and vulnerability scans. P-3 and P-4 stressed that most security solutions are reactive and used the antivirus as an example that protects against known threats and could leave the organization vulnerable to new threats. The situation increased the importance of performing vulnerability management to correct systems flaws. P-1 described vulnerability management as a recurrent task. P-5 and P-7 use a patch management system to install security updates. P-7 uses manual patching for servers to safeguard their availability. P-5 uses network access control to block or update computers out of compliance.

System and services acquisition. P-3, P-4, and P-8 recommended outsourcing technical support to ensure access to expert advice. P-5 and P-7 recommended including training vouchers as part of contracts to cover the technologies used by the municipality.

P-3 explained that technology changes so fast that is hard to keep staff up to date, whereas outsource services places the responsibility of training staff on the provider. P-4 recommended leveraging technologies that offer security, continuity, and redundancy. P-5 and P-8 recommended auctions and negotiation as vehicles to lower cost. Through negotiation, P-5 achieved cost saving of 50% less than what the state government pays for the same service. P-8 promoted centralized procurements to get wholesale prices. P-5 recommended including financial penalties as part of the service level agreement to prevent extended outages based on the provider's lack of responsiveness.

Information and Data

The information and data dimension was identified as the second most relevant to cybersecurity. This dimension was accredited by the participants as a fundamental input to support the organizational structure and processes dimension and related elements. Figure 7 displays the hierarchical position and the equal relevance of its elements.

Awareness and training management. Most participants use a combination of classroom, online, and external training to support SETA programs. P-4 explained that raising awareness can be as simple as sending an email but explained that it is not an easy task for technicians and recommended working with human resources (HR) to achieve a user-friendly format. P-5 mentioned that since HR is required by the comptroller to provide training, P-5 leverage the training for IT purposes. As low-cost alternatives, P-3 and P-5 recommended the using experienced employees in conjunction with a train the trainer model. P-5 also recommended developing user manuals as part of system

implementations that can be used for training. P-3 suggested a reimbursement option for dependencies to cover some of the costs. P-7 recommended the use of free tutorials.

As part of SETA programs, P-4, P-5, and P-7 advocated for continuing education (CE). P-7 described CE as a mutual commitment where the staff commits to study, and the employer provides the resources. P-7 included CE as part of the position's description but shared that HR was not used to the requirements. P-7 stated, “these requirements are needed as a tool for development and as an evaluation criterion that gives us an element that I can put in your evaluation.” P-7 also mentioned that the government does not see CE as an investment for IT professionals as it does for other professions. P-7 affirmed that it is hard to get a budget for CE, but CE is what provides the staff with the knowledge to do their jobs. P-7 explained, "the Oficina de Ética Gubernamental [Office of Government Ethics] required completing a determined amount of time every year on ethical training” and endorsed adopting a similar approach. P-1 and P-5 identified professional associations as a low-cost training option for CE.

Awareness training (AT). P-1 and P-4 identified users as the weakest point. P-1 recognized AT as a tool to promote awareness, strengthen commitment, and change the culture. The participants affirmed providing AT to new employees, but none provide recurrent training. Further, P-4 acknowledged that AT had not been given to everyone. P-4 explained that security tools are doing an excellent job preventing system-targeted attacks while user-targeted attacks are on the rise. P-7 mentioned that AT without security controls would not guarantee following the rules, but controls without AT can drive users to circumvent them. P-4 mentioned that users often do it unconsciously or

based on a false sense of security by assuming that established controls will protect them. P-4 stressed that users who were not trained should not be blamed for incidents.

P-7 explained the risk of information leakage such as PII which can be used for identity theft. P-1 stressed the need to change "the organizational culture that believes that because it has not happened, it will not happen." Similarly, P-7 mentioned that most people do not "realize the importance of cybersecurity until the day it hurts them." P-3 and P-7 agreed on the need to remind users and management about the current threats as well as to explain the impact these threats may have in the office and their homes. P-3 is confident that once "the person achieves that understanding, we get them to commit and support us." According to P-4, "awareness will result in prevention."

Operational information and role-based training. P-1 explained that often cybersecurity is not taken into consideration and mentioned developers who think of functionality instead of cybersecurity. P-3 affirmed, "the priority is to provide services that are accessible, secure and efficient." Therefore, cybersecurity training is crucial for technical staff. P-4 mentioned that without CE, cybersecurity professionals could be stuck with ineffective methods and will not be aware of new threats and mitigation. P-4 and P-6 also recommended attending conferences and collaborating with other organizations to share methodologies and practices. P-5 provided the example of ethical hacker training where most of the attendees, were thoughtful about their vulnerabilities and possible remediations. P-5 stated, "you can keep public servants focused on their work by giving them this type of knowledge and training." P-4 proposed sending staff to conferences to bring back information and follow-ups with the vendors as needed.

P-1 stated, “the education is the biggest challenge, and I do not mean technical, I am talking about upper management understanding that if we have to provide a service, it must be secured.” P-1, P-2, and P-5 recognized that often management lacks the knowledge about what needs to be implemented for cybersecurity. P-2 use news media to monitor cyberattacks and understand their characteristics, impact, and mitigations. P-2 mentioned that “it sounds weird, but cyber incidents and cyberattacks are the most influential factors to achieve a resilient cybersecurity posture.” P-4 agreed with P-2 and shared an incident that helped to increase awareness on the need for cybersecurity. P-2 recommended, “before presenting a proposal, came with a lesson to educate management” and justify the acquisition of new technologies to support cybersecurity.

Technology

The technology dimension was identified as a key enabler. The elements in this dimension support the element of the organizational structures and processes dimension. This dimension was also identified as the primary line of defense to protect and defend from the threats and challenges of the general context as well as insider threats.

Access control-technical. P-4 stated, “too many people, systems, and things coming out every day to try to enter and get information from your network,” and technology provides the capability to monitor the environment. P-7 identified technology as the vehicle to enforce access controls and reduces the attack surface. P-4 considers systems to be more reliable than users who might forget what they were taught. P-8 identified the technologies as the reason the municipality has “not suffered any

incidents." As part of the access management process, P-5 use technology to enforce policies, including expiration, complexity, and history, among others.

P-7 experienced incidents where "people who get very creative and get into web pages that they should not have, or bring a device infected with a virus." P-4 and P-5 use technology to enforce limited access to applications, the Internet, and social media based on user roles. P-4 explained that users must use the solutions that the municipality can secure. P-4 and P-7 recognized mobile devices as an area of concern as users with the ability to configure phones and the exposure of lost or stolen devices are a risk. P-7 has a mobile device management solution, while P-4 is testing alternatives to address the situation as well as to provide the capabilities to implement future cost-effective strategies such as bring your own device. As mitigation, P-4 uses an application to see the location of the devices and performed remote erase.

System and communications protection. The participants confirmed the use of boundary and cryptographic protection as the first line of defense, including unified threat management, firewalls, IPS, IDS, antispam, and traffic inspection. P-8 explained that boundary protection technologies help to enforce internal and external controls such as the routing of data leaving or entering the network. P-4 recommended using security layers starting with network-based at the boundary and host-based at the endpoint. P-3 and P-5 recommend the use certificates to protect websites and encrypt communications. P-5 and P-7 mentioned that the communication of their security and network devices are encrypted. P-5 uses demilitarized zone to restrict systems with direct access to the Internet and avoid the exposure of the internal network.

Summary

The central question of the study RQ1 was used to understand the perception of the participants on the readiness of government municipalities to protect and defend information resources. The result was of a positive connotation as participants perceived the posture of their municipality to be resilient. The participants agreed that their municipalities are more secure because of their ability to manage mature processes and leveraging supporting technologies. Nevertheless, the participants recognized having room to improve their cybersecurity program.

RQ2 focused on the elements influencing the municipal cybersecurity posture with the intent to provide a deeper understanding of the factors enabling or hindering their posture. The findings validated and added a layer of elements to the dimensions influencing digital government. The institutional framework and interorganizational collaboration dimensions failed to provide the foundation to support a resilient posture. The organizational structures and processes dimension was discovered to be key to a resilient posture while the elements of the information and technology dimensions were crucial to support the organizational structures and processes.

The upcoming chapter covers the interpretation of findings, including how the finding extended the body of knowledge and the relationship to the literature review. The chapter also includes a description of limitations to trustworthiness. In the same way, the chapter covered recommendations for future studies taking into consideration the strengths and limitations of the current research. Lastly, Chapter 5 is used to describe the potential impact for positive social change as well as the recommendations for practice.

Chapter 5: Discussion, Conclusions, and Recommendations

The purpose of this study was to understand the cybersecurity posture of municipal governments from the perceptions of public servants serving in IT leadership roles in Puerto Rico. I also attempted to identify the primary factors influencing the cybersecurity posture. The perception of this population originated from their lived experiences with different cybersecurity concepts. A qualitative approach was used to examine the lived experiences of IT leaders as information-rich cases.

The nature of this study was phenomenological. Transcendental phenomenology was appropriate for studying the cybersecurity posture of municipalities as a social problem. Most security artifacts are protected from public release by privacy laws like FOIA of 1966. However, individuals such as IT leaders are trustworthy and dependable alternate data sources that can be used to study the cybersecurity posture of municipal governments.

The central finding from the perceptions of the participants regarding the posture of their municipalities to protect and defend information resources was resilient. The participants pointed to the elements of organizational structures and process dimensions as the reason why their municipalities are more secure. Regarding the elements influencing the municipal posture, the findings added a layer to the dimensions influencing digital government, including areas such as technological changes, politics, economy, management support, and processes to achieve a resilient posture.

Interpretation of Findings

The findings of the study confirmed and expanded the information presented in the literature review. Regarding the security posture, the participants recognized that the posture was less resilient that the federal government, but more resilient than other municipalities and state agencies. Participants' perception was based on the maturity of their process and their ability to maintain technologies to support their cybersecurity operations. The findings also confirmed the dimensions influencing digital government as a valid framework to capture the complexity of the local government's cybersecurity posture. Further, analysis of the dimensions and the elements of the study from the lens of the OST confirmed that these components are interconnected, and changes in inputs, processes, outputs, feedback loops, and the environment can have positive or adverse effects on other components. Figure 10 shows the theoretical and conceptual framework as well as the results of the study to indicate the connection and influence of the different elements starting with a political interest in favor of a resilient cybersecurity posture.

Picazo-Vela et al. (2012) identified the economy, politics, and environmental factors as outputs of the general context. According to participants in the current study, most of these elements have a null or negative effect on their posture. For instance, the fiscal situation has a negative effect on the municipalities' ability to manage resources to support cybersecurity. Saxby (2015) identified technology investments as a significant challenge, particularly for small entities. However, economic growth by itself could have a null effect as other elements such as cyber threats or political interest will be required to achieve a positive response.

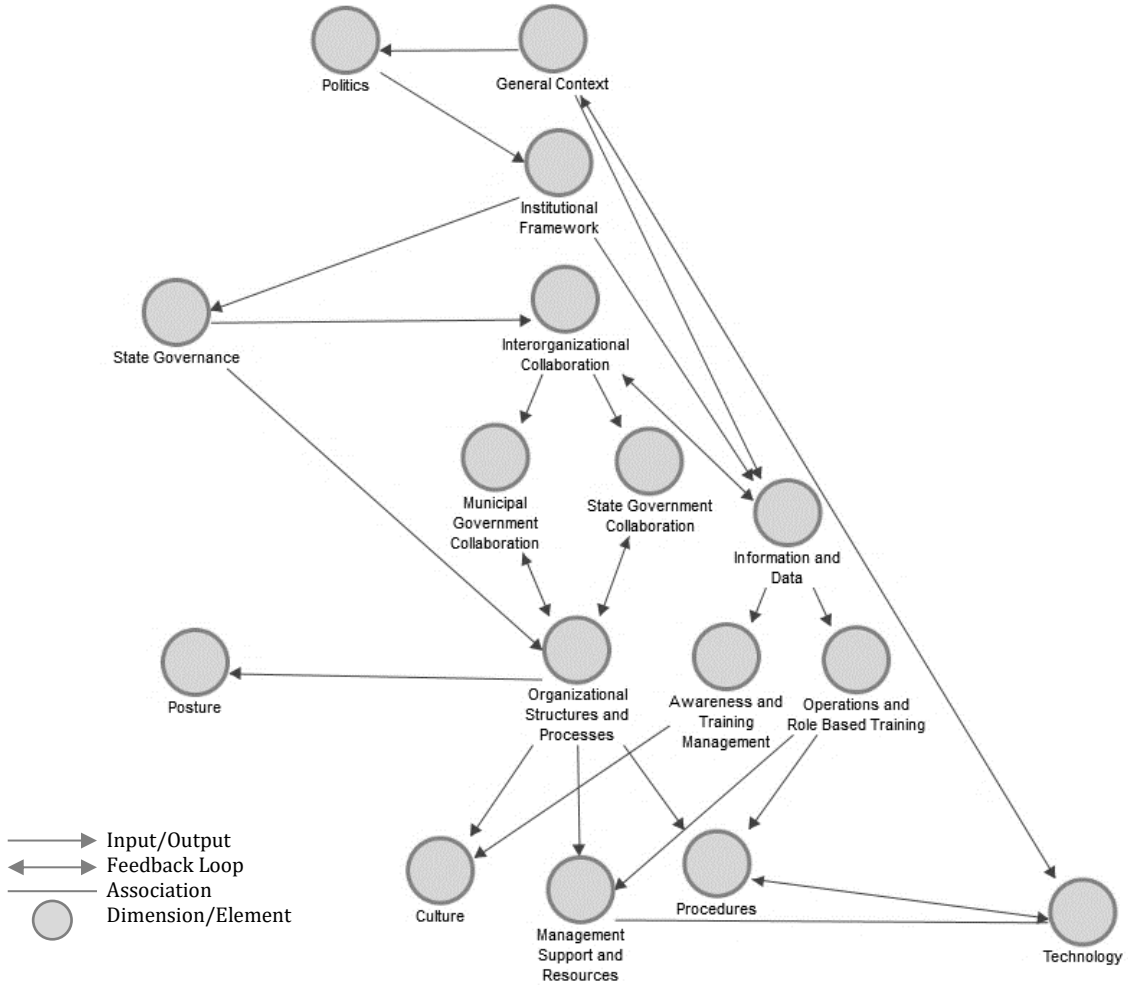

Figure 10. Concept map of political interest influence on cybersecurity. This figure combines the theoretical and conceptual frameworks with the results of the study to show the relationship and influence of the different elements affecting the local government cybersecurity posture.

Cyber threats and new technologies were identified as primary technological changes affecting cybersecurity. Kenney (2015) mentioned that attackers use similar strategies. The participants in the current study identified ransomware, phishing emails, and website spoofing as common strategies. Regarding the actors, Fok (2015) divided attackers into several groups: hackers, amateurs, script kiddies, and people with technical skills looking for "fun or notoriety" (p. 33). According to participants in the current

study, attackers are their main threat. In addition to the threat environment, the evolution of technology has also brought new challenges. For instance, the participants recognized that the increased adoption of the Internet had resulted in an increased demand for online services as well as systems to support mobility and data-driven business processes. These systems and services increase the attack surface and exposure risk of the municipalities.

Politicians are negatively affecting cybersecurity by not recognizing it as a priority. The political factor reflected in the finding is nourishing division, repetition, and lack of cross-government interoperability creating additional challenges. Private sector interest is focused on eliminating the competition and making a profit. These interests had also resulted in a degradation of infrastructure and a monopolized market. On the contrary, a political interest that prioritizes cybersecurity can serve as an input to the institutional framework influencing the process to develop and implement policies. Likewise, a positive private interest could influence the institutional framework or interorganizational collaboration to develop or adopt cybersecurity standards.

The institutional framework is limited to state governance including the E-Government Act of 2004 and circulars covering high-level requirements without adequate guidance. The participants reported that the policies are not well communicated, nor readily accessible, and are not available in a format that presents changes and current applicability. I confirmed these conditions during the literature review process. Federal guidelines can provide the body of knowledge, frameworks, and standards to manage cybersecurity. However, most participants expressed a lack of familiarity with federal policies as the participants follow best practices and the comptroller's guidance, which

does not include federal or international standards. Kazemi et al. (2012) identified complying with standards as a crucial factor for a successful security program.

The comptroller is responsible for performing IT audits, but these are done infrequent manner and do not have a clear scope, plans, or metrics. The last audit was done in 2016. Roesener et al. (2014) found that government agencies' roles and responsibilities are often overlapping and lacking the necessary authority. These results are aligned with the situations of the CIO of Puerto Rico. The CIO has been deprecated and reenacted in recent years. Reestablished in 2017, the CIO has focused on state agencies instead of adopting a cross-government approach to develop solutions, foster collaboration, and facilitate information sharing. Elements such as political interest can influence the institutional framework to mandate cybersecurity standards and require collaboration through policies. The policies can serve as the input driving the need for a cross-government collaboration process.

According to the results of the study, collaboration with the federal, state, and municipal governments was limited to emergency response or other compulsory conditions, while collaboration with the private sector was limited to contractual relationships. Gil-Garcia and Pardo (2005) mentioned that government entities tend to act independently failing to contemplate what is being done by others. Scholars agreed that the government alone cannot secure cyberspace and needs the support and collaboration of other sectors (Clinton, 2015; Hiller & Russell, 2013; Hua & Bapna, 2013; Miron & Muita, 2014; Roesener et al., 2014).

The participants acknowledged the importance of collaboration and shared their willingness to collaborate, but most looked at the state government as the one responsible for facilitating the conditions. Clinton (2015) identified policy as a vehicle to require cross-sector collaboration, particularly to facilitate "a common understanding around various risk management terms, methodologies, ideas, and language" (p. 67). One of the participants agreed with Clinton regarding shared planning to perform benchmarking with cross-sector organizations. The information shared in this dimension will serve as input and feedback loop to influence the organizational structures and processes.

The capabilities to prevent and respond to cyberattacks are related to the organization's structures, resources, technologies, and policies. Armbruster et al. (2013) discovered that the implementation of organizational processes is more challenging for decentralized IT departments. Flores et al. (2013) also identified centralization as an efficient structure. Participants in the current study confirmed these findings by identifying centralization as the most effective structure to manage cybersecurity resources and access controls. The people, their roles, and their responsibilities are also essential parts of the organizational structure. Reece and Stahl (2015) stressed the need for a managerial role such as the CISO to manage cybersecurity. The participants agreed but shared that cybersecurity is managed as a secondary role instead of a primary function. The lack of a cybersecurity manager was identified as a lesson learned from a cyberattack against Hacienda (Minelli-Pérez, 2017). The participants associated the absence of dedicated cybersecurity resources with the lack of personnel due to the fiscal situation.

Scholars agreed on the importance of understanding the organizational culture (Flores et al., 2013; Kazemi et al., 2012). Participants in the current study mentioned that the concept of cybersecurity is new and is not part of the culture, which leads to it often being overlooked. According to Nugent and Collar (2015), organizational culture fails to perceive cybersecurity professionals as heroes protecting the network. Some of the participants described cybersecurity professionals as silent heroes who work to prevent incidents. Participants also mentioned that cybersecurity professionals are often seen as bad guys for restricting access as part of the security controls. Kazemi et al. (2012) identified management support as one of the top seven factors to achieve a successful information security program. Management recognition of cybersecurity professionals can have a positive effect on job satisfaction and user awareness of cyber threats. Current study participants agreed that management support is crucial to the assignment of resources to support cybersecurity operations. Most participants shared having a good experience with management while others reported challenges associated with their understanding of security requirements and resources assignment.

The participants shared a vast experience of organizational processes aligned with best practices such as the Center for Internet Security (CIS) Controls (see Figure 11) and high-level federal standards such as FIPS 200 (see Table 2). The main processes in order of relevance were related to contingency planning, System and information integrity, access control, risk assessment, system and services acquisition, and configuration management. The frequent exposure to hurricanes made contingency planning and related subprocesses critical to municipal IT operations. Armbruster et al. (2013)

explained that 71% of organizations who tested their contingency planning discovered problems during the testing that could have happened during a real situation. Current study participants identified testing as vital to the success of their contingency planning. The participants also mentioned having alternate processing and storage sites, as well as redundant telecommunication. System backup was identified as another crucial strategy to recover from natural or humanmade incidents. On 2017, lack of proper system backup caused Hacienda to lose 50 terabytes of data after an attack (Minelli-Pérez, 2017).

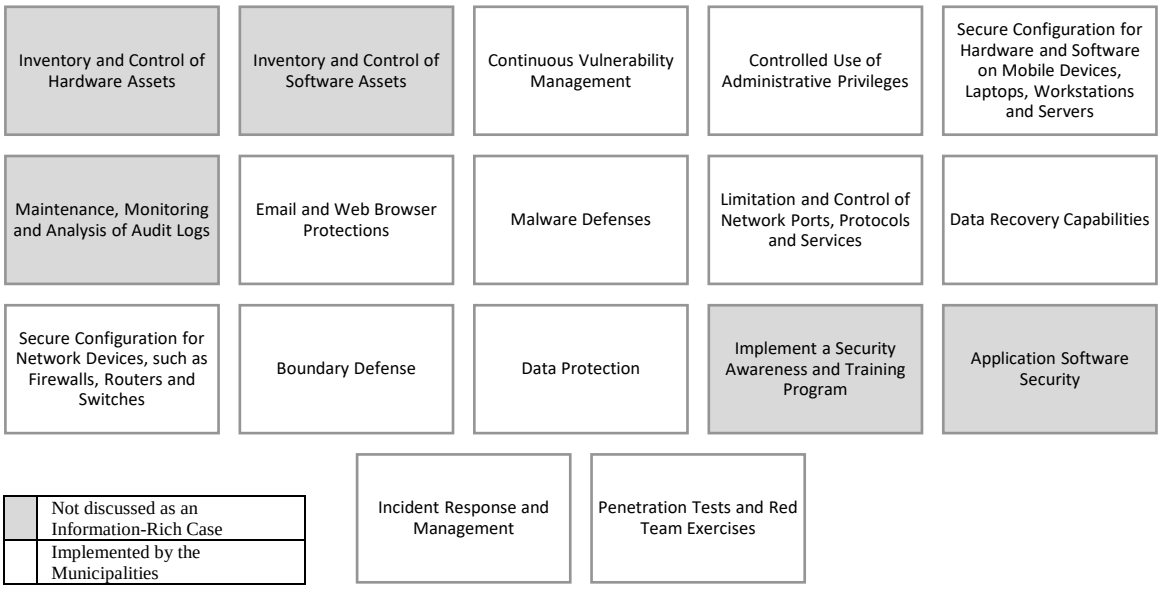

Figure 11. CIS controls best practices and local government posture. This figure shows the relationship between cybersecurity best practiced and the practices followed by the municipalities that participated in the study.

Participants and scholars agreed on the importance of system and information integrity to perform vulnerability management and malicious code protection. The participants shared using centralized antimalware solution and managing vulnerabilities through a combination of manual and automated processes. Access control processes were used for account management and to control access based on roles. The participants

also acknowledged performing risk assessment such as vulnerability assessments and penetration testing. Hua and Bapna (2013) mentioned the use of cost-effective investments to improve resiliency. The participants are using system and services acquisition to cover security requirements such as service support for their security tools and leveraging the security capabilities of the providers. Configuration management is used by the participants to limit and control configurations, ports, protocols, and services.

The information dimension serves as inputs and feedback loops to provide awareness and role-based understanding to stimulate the culture, improve processes, and empower management. Most participants use a combination of classroom, online, and external training to support SETA programs. Adams and Makramalla (2015) shown that 80% of exploits are related to the human element. Participants identified end users as the weakest link and recognized AT as a tool to promote awareness, strengthen commitment, and change the culture. The participants recommended cost-effective alternative including sending email, using experienced employees as facilitators, using a train the trainer model, developing user manuals as part of system implementations that can be used for training, using free tutorials, and leveraging professional associations. Douba et al. (2014) affirmed that there is a relationship between digital literacy and cyber resiliency. Therefore, it is crucial for technical staff to the benefit of CE in the form of training, conferences, and networking to share methodologies and practices.

The priority of the participants providing services that are accessible, secure, and efficient. Participants identified technology as the enabler to enforce access controls and reduce the attack surface. Systems are considered more reliable than users who might

forget what they were taught. Therefore, technology is used to enforce password policies, including expiration, complexity, and history as well as to limit access to applications, the Internet, and social media based on roles. Technology serves as the primary line of defense to protect and defend from the threats of the general context as well as insider threats. All of the participants confirmed the use of boundary and cryptographic protection, including unified threat management, firewalls, IPS, IDS, antispam, and traffic inspection. Scholars agreed that these technologies are essential to prevent and respond to cyberattacks (Hua & Bapna, 2013; Levesque et al., 2015).

Delimitations

The delimitations of the study consisted of exploring the local government readiness to protect and defend information and systems within the San Juan – Carolina – Caguas MSA. The scope of the study also included analyzing the influential factors to the management of information resources and security controls. Patton (2002) described the purpose of delimitation as a method to focus on data more relevant to the problem been studied. For this reason, the sampling strategy excluded participants from less populated municipalities and concentrated on public servants working in IT leadership roles within the San Juan – Carolina – Caguas MSA as information-rich cases. OST served as the theoretical foundation to study the municipal posture as an open system influenced by its interactions with the external environment. Additionally, the dimensions influencing digital government was the conceptual framework used to identify the dimensions and elements of the external environment affecting the municipal cybersecurity posture. These delimitations helped to understand the different elements affecting the

phenomenon to facilitate the development of strategies to improve the cybersecurity resiliency of local government agencies.

Limitations of the Study

The limitations of the study were identified as the sampling strategy, the dependability of the data, and the availability of the participants. The purposeful sampling strategy concentrated in public servants in IT leadership roles within highly populated municipalities. The strategy proved to be effective as the participants served as information-rich cases. However, it would have been beneficial to include the perception of IT leaders within not highly populated municipalities. Another limitation was not collecting demographic information from the participants to preserve their confidentiality. Not having this information prevented from performing correlations of the results with factors such as the age or education of the participants.

Regarding the dependability of the data, there was limited literature about cybersecurity at the local government level. Therefore, the literature was focused on national and state government levels within the United States. The primary data related to the local government was collected from interviews. The criterion sampling included at least 2 years of experience with the phenomenon which proven to increase the dependability of the data. The experience of the participants with the phenomenon and their experience with the elements affecting their cybersecurity posture was crucial to the study.

The availability of the participants had the strongest impact on the study. In late September of 2017, a Category 5 hurricane devastated Puerto Rico. This situation

increased the participant's experience in disaster recovery efforts but affected their availability to participate in the study. The municipalities of Toa Baja and Toa Alta were planned to be invited to participate, but due to the situation with the hurricane were unreachable. Also due to availability constraints, 10 participants were interviewed, but two of the eight interviews were done with two participants at the time where one participant was the primary interviewee while the other played a supporting role. The sample remained within the range of five to 25 participants as recommended by Creswell (2013).

Recommendations

Several recommendations emerged from the execution of this study. The purpose of these recommendations is to be used to further research on cybersecurity posture as a phenomenon of inquiry. The recommendations are based on the strengths and limitations of the study, including theory, scope, limitations, and methodology. The theoretical foundation was OST which originated from the GST. Sher (2004) explained that GST focuses on the arrangements, functions, and relationships among the elements of a system. In addition to the relationships, Shafritz et al. (2015) considered the elements of a system to include “inputs, processes, outputs, and feedback loops, and the environment” (p. 340). These principles served as a strength to the outcome of the study as it facilitated the understanding of the relationships and functions of the dimensions and elements affecting cybersecurity. Therefore, OST is recommended for future studies.

The conceptual framework also demonstrated to be useful to study cybersecurity. Since there was a significant knowledge gap about cybersecurity at the local government

level, the dimensions influencing digital government was used to provide an understanding of the different constructs that could affect the phenomenon. The conceptual framework consisted of six dimensions, including general context, institutional framework, interorganizational collaboration, organizational structures and processes, information and data, and technology. It is recommended for further studies to focus on individual dimensions or a set of related dimensions. Based on the data collected from the participants and the literature review, further research related to the institutional framework and organizational structures and processes could be beneficial to continue to bridge the knowledge gap about this phenomenon.

The scope and delimitations of the study were justifiable and necessary to gain as much knowledge as possible about cybersecurity at the local government. The research design leveraged purposeful focused on IT leadership roles in highly populated municipalities. The environment of these municipalities as expected increased the participants' exposure and experience with the phenomenon allowing them to serve as information-rich cases. According to the participants, their municipalities were perceived to be more resilient than smaller municipalities and state agencies. Participant in IT leadership roles should remain the unit of analysis. However, future studies should include participants from less populated settings to understand their perception of the cybersecurity posture and the elements affecting their posture. A similar approach could be used to study state agencies, in particular, those responsible for critical services such as Hacienda, OGP, Puerto Rico Electric Power Authority and Puerto Rico Aqueducts and Sewers Authority, among others.

The sampling strategy included criterion sampling as a "predetermined criterion of importance" (Patton, 2002, Criterion sampling, para. 1). The criteria used in the study included participants working in IT leadership role or performing related functions with at least 2 years of experience working within highly populated municipalities. This strategy was crucial to the dependability of the data. It is recommended to use a similar criterion in further studies. One of the weaknesses of the study was that personnel meeting this criterion have limited availability to participate in studies. The data collection process consisted of in-person interviews with the purpose of having a more direct interface with the participants to help foster confidence and collaboration to provide as much data as possible. Future studies could use video conference technologies to conduct the interviews or use a combination of video conference and in-person interviews based on participants availability.

Creswell (2013) narrative, phenomenological, grounded theory, ethnographic, and case study as the main qualitative research traditions. This study used a phenomenological approach to understand the cybersecurity posture and influential its elements as a multidimensional phenomenon from the lived experience of the participants. Further research concentrated in a particular dimension could use a case study approach. Creswell described the case study methodology as exploring a real-life bounded system. For instance, a case study could be used to research state governance within institutional framework dimension as it relates to the comptroller's IT audit of 2016 in Puerto Rico as a bounded system while municipalities or state agencies could serve as the unit of analysis for the study. Similarly, processes such as contingency

planning within the organizational structures and processes dimension could be used to study the impact of hurricane Maria in 2017 over state or local government IT operations.

Puerto Rico's government and institutional framework resemble that of a U.S. state. The U.S. states also share other elements of the general context such as economic challenges and threats both human or natural. For instance, states like Florida, Louisiana, Texas, and the Carolinas have been impacted by major hurricanes. Based on these conditions, is also recommended conducting a replication or variation of this study in a U.S. state to explore the cybersecurity posture of their local governments.

Implications

Implications to Social Change

The results of the study serve to raise awareness of cyberattacks as a social problem affecting individuals and organizations. Advances in technology have led to technical solutions capable of protecting against system-targeted attacked. Meanwhile, user-targeted attacks continue to increase. Phishing emails are the most common attack directed at individuals at their homes and workplaces with the intent to make the receiver respond with sensitive information or executing a malicious payload such as ransomware. The sensitive information is used to conduct identity theft or gaining access to financial assets while ransomware encrypts all the data in the infected system and asks for a ransom for the encryption key. Ransomware can spread into interconnected systems. If the incident happened at a government agency, individual and families might not be able to receive most needed services.

Similarly, government operations can be affected by cyberattacks as well as natural disaster. Both cases can result in social and economic injustice to individuals and communities within the affected jurisdiction. In addition to raising awareness, the implications of the research contribute to positive social change by providing advance knowledge to support future investigations and by empowering individuals and organizations with expert knowledge about the essential elements to support a resilient cybersecurity posture. Increasing awareness on cyber threats and sharing an understanding of the elements to manage their risks can lead individuals and organizations to adopt an active role to improve their posture and support public safety.

Implications to Theory

The main methodological implication was the usefulness of the of the research approach and its influence on the research design. Phenomenology was proven to be an effective methodology to study cybersecurity as a social problem. Cybersecurity data at an organizational level is protected from public release which difficult most quantitative strategies. Other qualitative methodologies such as case study could have made the participants hesitant to engage in the research as their organizations could be affected by the results. However, phenomenology made available data significant to the problem through the perception and lived experiences of the participants. This approach increased the need to access information-rich cases which drove the purposeful criterion sampling strategy. Phenomenology also led to the selection of face to face interviews with open-ended questions to establish a connection with the participants to allow them to share as most information as possible.

The theoretical implications included the application of OST and the dimensions influencing digital government conceptual framework as the theoretical lenses to interpret the findings. Dimensions influencing digital government divided the environment into six dimensions. Within each dimension, different elements were identified. The conceptual framework provided a deep understanding of the function of these elements and a brief understanding of their relationship. OST was able to augment this understanding by identifying the elements' relationships and influence over one another as inputs, processes, outputs, and feedback loops within the environment.

The contribution the body of knowledge is the most significant empirical implications. Part of the purpose of this study was understanding the cybersecurity posture of the local governments and identifying the factors influencing their posture with the intent to bridge the knowledge gap about this phenomenon. Literature about the phenomenon was limited to national and international settings. The results of this study contributed to the body of knowledge by providing research-based data addressing gap about cybersecurity at the local governments. The dimension and elements affecting cybersecurity and their relationship were identified as part of the study. This empirical data can serve as the foundation for future investigations.

Implications to Practice

The implications to practice are related to the findings discovered within the elements of the dimensions influencing digital government. The implications can help to provide awareness of the general context, tools to strengthen the institutional framework, alternative for interorganizational collaboration, information resources, and technology

management. The results of the study can also benefit the municipalities to leverage the elements of the institutional framework, information and data, and technology dimensions to improve organizational structures and processes.

From the general context, technological changes particular to the threat environment were identified as the primary challenge. The U.S. Computer Emergency Readiness Team (n.d.) manages the National Cyber Awareness System. This system consists of five products including Alerts, Analysis Reports, Bulletins, Current Activity, and Tips to inform the government, private sector, and the general population about cyber threats and mitigations. IT staff, as well as nontechnical staff, can register to receive notifications for the areas interest to maintain awareness on the threat environment. Regarding positive or negative influence from elements such as the economy, politics, and private interest can be managed with processes within the organizational structures and processes dimension.

According to the results of the study, there is a significant gap in the institutional framework. The Government of Puerto Rico can use existing federal governance as the foundation to improve their current policies. For instance, the state government could use FISMA of 2014 as a guiding source to update the E-Government Act of 2004. Similarly, the Government of Puerto Rico could use OMB Circular A-130, *Managing Federal Information as a Strategic Resource* to update or consolidate current circulars. The state and municipal governments could use FIPS 200 to guide the development of uniform minimum security requirements.

According to the results of the study, the government security requirements and the scope of the comptroller's IT audit were not clear. The state government including the comptroller and the CIO of Puerto Rico could adopt NIST SPs as guidelines to support cybersecurity activities across the government. SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* could help to develop minimum security requirements into manageable security controls. In the same way, the comptroller could use SP 800-171A, *Assessing Security Requirements for Controlled Unclassified Information* to develop clear audit scope, plans, and metrics.

Regarding standards and best practices, the participants identified that municipalities follow best practices and limit the implementation of standards to those required by the comptroller. Most standards could be expensive to implement, including the cost to access their related information. However, NIST guidelines are free to the public and are aligned with Committee for National Security Systems and international standards such as "ISO/IEC 27001, *Information technology–Security techniques–Information security management systems–Requirements* and ISO/IEC 15408, *Information technology -- Security techniques -- Evaluation criteria for IT security"* (Joint Task Force Transformation Initiative, 2013, p. H-1). The Federal Trade Commission offers free access to best practices endorsed by the government that is available in English and Spanish (Federal Trade Commission, 2018). In the same way, CIS offers community developed best practices with some of the documentation available in English and Spanish (CIS, 2018). The resources in the institutional framework can be

used by IT leaders and policymakers to raise awareness, develop, and implement detailed policies in alignment with national and international cybersecurity practices.

The absence of collaboration was identified as an area of concern. Outside compulsory conditions, no collaboration with the federal government was identified. NICE is a federal program consisting of "a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development" (NIST, 2018, p. 1). NICE serves as a collaboration platform for local, state, and federal governments. State and municipal government entities could join NICE' workgroups to benefit from the collaboration activities and start networking efforts with other government entities. The state government could use the institutional framework to buoy up interorganizational collaboration or appoint the CIO as the responsible entity to establish a collaboration platform that includes the local governments. Also, the municipal government could establish collaboration initiates with neighboring municipalities, local academic institution, and the private sector.

The organizational structures and processes reflect the organizational posture by using its structure, roles, and procedures to protect information and systems from the challenges and threats of the general context, comply with the institutional framework, and advance operation by using interorganizational collaboration, information, and technology as feedback loops. For instance, information about the threat environment such as the one provided by the U.S. Computer Emergency Readiness Team can help prepare to defend and protect the organizational against current threats as well as to gain management support by justifying the need for technologies or personal to support

cybersecurity operations. Economic situations such as the current fiscal crisis can be detrimental to cybersecurity operation. However, long-term capital planning, centralized procurement, contract negotiation, and Agile project approach can help to reduce cost and improve the management of available resources.

The results of the study shown that cybersecurity is treated as a secondary role. Cybersecurity is a complex domain composed of multiple operational processes related to access control, configuration management, contingency planning, risk assessment, system and services acquisition, and system and information integrity, among others. Failing to have dedicated resources to make sure that the processed are defined, implemented, and managed will have an adverse effect on the cybersecurity posture. In the absence of a dedicated cybersecurity professional, the information and technology dimensions are crucial to mitigate the situation. AT is crucial to raise awareness, change the culture, and give the users the tools to help protect the organization from cyber threats. Municipalities should include AT for every new user as well as yearly as a reminder to existing users. The participants recommended that the central government develop and make available the training to reduce duplicative effort and related cost.

Similar to AT, role-based training is fundamental to maintained technical staff up to date, especially when the technical staff working with cybersecurity as a secondary function. As recommended by the participants, CE should be part of the position description and encourage by the employer. The municipalities could use online courses, webinars, conference, formal courses, professional associations, and resources from the interorganizational collaboration dimension to make sure the staff is well equipped with

the information necessary to safeguard the organization through the management of cybersecurity-related processes and technologies.

Technology is the central defense against threats and the mechanism to implement access controls. Therefore, it is crucial for these tools to be properly configured. Security technical implementation guides are the configuration standards developed by Defense Information Systems Agency (n.d.) to harden against attacks. CIS offers similar guides refer to as Benchmarks that can also be used to configure technologies securely (CIS, 2018). These guides are free to the public. Municipalities can leverage these guides to configure their technologies to be resilient against cyberattacks.

Conclusions

Cyberspace is a new domain that policies have not been able to address with success. Policies like FISMA of 2014 assign responsibilities to federal agencies, while leaving state and local governments without a legal obligation and resources to protect their information and systems while putting their operations and the wellbeing of their constituents at risk. At the same times, advances in technology and constituents demand continue to drive the implementation of online services. Kazemi et al. (2012) explained that the increasing dependency on these technologies is reflected on the upsurge of cyber threats.

In addition to increasing the exposure to cyber threats, the interconnectivity within cyberspace increased the risk to compromise interconnected systems. Therefore, the compromised of a municipal or state system could jeopardize the confidentiality, integrity, and availability of other interconnected municipal, state, or federal systems.

Municipal governments use the same types of sensitive information as other government entities. Municipalities also serve as first responders, critical infrastructure providers, and are responsible for local economic development (Miron & Muita, 2014; Sylves, 2015). Therefore, risks against their IT infrastructure can cause social and economic injustice to the individuals and communities in their jurisdiction. It is critical that public servants understand the factors influencing the cybersecurity posture of their agencies.

The results of this study contributed to the body of knowledge to bridge the gap between in literature, theory, and practice. The results of the study provided information on the challenges and strategies related to the cybersecurity posture of the local government based on the perception of committed IT leaders who work to protect their organizations from cyber incidents while delivering accessible, secure, and efficient services to support the mission of their municipalities and their constituents. The outcome of the study validated the applicability of the OST and the dimensions influencing digital government as theoretical lenses to study the phenomenon while expanding the conceptual frameworks to include additional elements affecting cybersecurity and their relationships. The results of the study also provided research-based solutions to empower practitioners with the knowledge to improve the different elements affecting cybersecurity with the goal to achieve a resilient cybersecurity posture.

References

Adams, M., & Makramalla, M. (2015). Cybersecurity skills training: An attacker-centric gamified approach. *Technology Innovation Management Review, 5*(1), 5-14. doi:10.22215/timreview/861

Armbruster, G., Endicott-Popovsky, B., & Whittington, J. (2013). Threats to municipal information systems posed by aging infrastructure. *International Journal of Critical Infrastructure Protection, 6*(3-4), 123-131. doi:10.1016/j.ijcip.2013.08.001

Asllani, A., White, C. S., & Ettkin, L. (2013). Viewing cybersecurity as a public good: The role of governments, businesses, and individuals. *Journal of Legal, Ethical and Regulatory Issues, 16*(1), 17-14.

Bailey, K. (2005). General systems theory. In G. Ritzer (Ed.), *Encyclopedia of social theory* (pp. 310-316). Thousand Oaks, CA: SAGE Publications, Inc. doi:10.4135/9781412952552.n117

Baker, V. (2013). *Information sharing among public safety agencies* (Unpublished doctoral dissertation). Walden University, Minneapolis, MN.

Bertot, J. C., Seifert, J., & Jaeger, P. (2015). Securing the homeland in the digital age: Issues and implications for policy and governance. *Government Information Quarterly, 32*(2), 105-107. doi:10.1016/j.giq.2015.04.001

Burgess-Allen J., & Owen-Smith V. (2010). Using mind mapping techniques for rapid qualitative data analysis in public participation processes. *Health Expectations, 13*, 406-415. doi:10.1111/j.1369-7625.2010.00594.x

Burke, W. W. (2011). *Organization change: Theory and practice*. (3rd ed.). Thousand Oaks, CA: SAGE Publications, Inc. [Kindle Cloud Reader version]. Retrieved from Amazon.com

Caruson, K., MacManus, S. A., & McPhee, B. D. (2012). Cybersecurity policy making at the local government level: An analysis of threats, preparedness, and bureaucratic roadblocks to success. *Journal of Homeland Security & Emergency Management, 9*(2), 1-22. doi:10.1515/jhsem-2012-0003

Center for Internet Security. (2018). Cybersecurity best practices. Retrieved from https://www.cisecurity.org/cybersecurity-best-practices/

Central Intelligence Agency. (2016). Puerto Rico. In the World Factbook. Retrieved from https://www.cia.gov/library/publications/the-world-factbook/geos/rq.html

Chen, H., & Dongre, R. (2014). Q&A. What motivates cyber-attackers? *Technology Innovation Management Review, 4*(10), 40-42. doi:10.22215/timreview/838

Clinton, L. (2015). Best practices for operating government-industry partnerships in cyber security. *Journal of Strategic Security, 8*(4), 53-64. doi:10.5038/1944-0472.8.4.1456

Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030 (1986).

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review, 4*(10), 13-21. doi:10.22215/timreview/835

Creswell, J. W. (2013). *Qualitative inquiry and research design: Choosing among five approaches* (3rd ed.). Thousand Oaks, CA: SAGE Publications, Inc. [Kindle

Cloud Reader version]. Retrieved from Amazon.com

Defense Information Systems Agency. (n.d.). Security technical implementation guides (STIGs). Retrieved from https://iase.disa.mil/stigs/Pages/index.aspx

Douba, N., Rütten, B., Scheidl, D., Soble, P., & Walsh, D. (2014). Safety in the online world of the future. *Technology Innovation Management Review, 4*(11), 41-48. doi:10.22215/timreview/849

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in smart cities: Safety, security and privacy. *Journal of Advanced Research,5*(4), 491-497. doi:10.1016/j.jare.2014.02.006

Exec. Order No. 13636, 3 C.F.R. (2013).

Executive Office of the President. (2013, February 13). Presidential Policy Directive-21 Critical Infrastructure Security and Resilience (PPD-21). Washington, DC.

Federal Information Security Modernization Act of 2014, 44 U.S.C. §§ 3551-3558 (2014).

Federal Trade Commission. (2018). Consejos [Tips & Advice]. Retrieved from https://www.ftc.gov/es/consejos

Flores, W. R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security, 43*, 90-110. doi:10.1016/j.cose.2014.03.004

Freedom of Information Act of 1966, 5 U.S.C. § 552 (1966).

Fok, E. (2015). Cyber security challenges: Protecting your transportation

management center. *Institute of Transportation Engineers Journal, 85*(2), 32-36.

Gil-Garcia, J. R. & Pardo, T. A. (2005). E-government success factors: mapping practical tools to theoretical foundations. *Government Information Quarterly, 22*(2), 187–216. doi:10.1016/j.giq.2005.02.001

Gil-Garcia, J. R., Pardo, T., & Baker, A. (2007). Proceedings from Hawaii International Conference on System Sciences (HICSS) '07: Understanding context through a comprehensive prototyping experience*: A Testbed Research Strategy for Emerging Technologies*. Waikoloa, HI. doi:10.1109/HICSS.2007.582

Google (n.d.). Stronger security for your Google Account: How it protects you. Retrieved from https://www.google.com/landing/2step/#tab=how-it-protects

Hiller, J. S., & Russell, R. S. (2013). The challenge and imperative of private sector cybersecurity: An international comparison. *Computer Law & Security Review, 29*(3), 236-245. doi:10.1016/j.clsr.2013.03.003

Hua, J. & Bapna, S. (2013). The economic impact of cyber terrorism. *The Journal of Strategic Information Systems, 22*(2), 175-186. doi:10.1016/j.jsis.2012.10.004

Jiang, J. & Klein, G. (2000). Software development risks to project effectiveness. *Journal of Systems and Software, 52*, 3–10. doi:10.1016/S0164-1212(99)00128-4

Johnson, R., L. (2012). *An Analysis of IT Governance Practices in the Federal*

Government: Protecting U.S. Critical Infrastructure from Cyber Terrorist Attacks. (Unpublished doctoral dissertation). Walden University, Minneapolis, MN.

Joint Task Force Transformation Initiative. (2013). Security controls for federal information systems and organizations (NIST Special Publication 800-53 Revision 4). National Institute of Standards and Technology. Retrieved from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Kadivar, M. (2014). Cyber-attack attributes. *Technology Innovation Management Review, 4*(11), 22-27. doi:10.22215/timreview/846

Kazemi, M., Khajouei, H., & Nasrabadi, H. (2012). Evaluation of information security management system success factors: Case study of municipal organization. *African Journal of Business Management*, 6(14), 4982-4989. doi:10.5897/AJBM11.2323

Kenney, M. (2015). Cyber-terrorism in a post-Stuxnet world. *Orbis, 59*(1), 111-128. doi:10.1016/j.orbis.2014.11.009

Kissel, K. (Ed.). (2013). Glossary of key information security terms (NIST Interagency or Internal Report 7298, Revision 2). Gaithersburg, MD: National Institute of Standards and Technology. doi:10.6028/NIST.IR.7298r2

Kostyuk, N. (2014). International and domestic challenges to comprehensive national cybersecurity: A case study of the Czech Republic. *Journal of Strategic Security, 7*(1), 68- 82. doi:10.5038/1944-0472.7.1.6

Levesque, R., Walsh, D'A., & Whyte, D. (2015). Securing cyberspace: Towards an agenda for research and practice. *Technology Innovation Management Review*, 5(11): 26–34. doi:10.22215/timreview/943

Levy, J. M. (2012). *Contemporary urban planning* (10th ed.). [Kindle Cloud Reader version]. Upper Saddle, NJ: Pearson Education Inc. Retrieved from Amazon.com

Ley de Gobierno Electrónico de 2004 [E-Government Act of 2004], 3 L.P.R.A. § 991 (2004)

Ley de Certificados y Comprobantes Electrónicos [Certificates and Electronic Receipts Act], 3 L.P.R.A. § 8721 (2009).

Ley de Ética Gubernamental de Puerto Rico de 2011 [Ethics in Government Act of 2011], 3 L.P.R.A. § 1854 (2011).

Lozowski, D. (2014). Cybersecurity: The challenges of interconnectivity. *Chemical Engineering, 121*(4), 5. Retrieved from https://www.chemengonline.com/cybersecurity-the-challenges-of-interconnectivity

Lozowski, D. (2015). Cybersecurity: Aligning priorities. *Chemical Engineering, 122*(4), 5. Retrieved from https://www.chemengonline.com/cybersecurity-aligning-priorities/

MacManus, S. A., Caruson, K., & McPhee, B. D. (2013). Cybersecurity at the local government level: Balancing demands for transparency and privacy rights. *Journal of Urban Affairs, 35*(4), 451-470. doi:10.1111/j.1467-9906.2012.00640.x

Maheux, B. (2014). Assessing the intentions and timing of malware. *Technology*

Innovation Management Review, 4(11), 34-40. doi:10.22215/timreview/848

Manley, M. (2015). Cyberspace's dynamic duo: Forging a cybersecurity public -private partnership. *Journal of Strategic Security*, *8*(5). doi:10.5038/1944 -0472.8.3S.1478

Maxwell, J. A. (2013). *Applied Social Research Methods Series: Vol. 41*. Qualitative research design: An interactive approach (3rd ed). Thousand Oaks, CA: SAGE Publications, Inc. [Kindle Cloud Reader version]. Retrieved from Amazon.com

Miles, M. B., Huberman, A. M., & Saldana, J. (2014). *Qualitative Data Analysis: A Methods Sourcebook* (3rd ed.). Thousand Oaks, CA: SAGE Publications, Inc. [Kindle Cloud Reader version]. Retrieved from Amazon.com

Minelli-Pérez, S. (2017). Luis Arocho hace énfasis en la ciberseguridad [Luis Arocho emphasizes cybersecurity]. *El Nuevo Dia*. Retrieved from http://www.elnuevodia.com/negocios/economia/nota/luisarochohaceenfas isenlaciberseguridad-2299582/

Miron, W., & Muita, K. (2014). Cybersecurity capability maturity models for providers of critical infrastructure. *Technology Innovation Management Review, 4*(10), 33–39. doi:10.22215/timreview/837

Moore, M. (2014). *Development and implementation of government cybersecurity policies and practices for national security and cybercrime*. (Unpublished doctoral dissertation). Walden University, Minneapolis, MN.

Morrell, J. (2005). Complex adaptive systems. In S. Mathison (Ed.), Encyclopedia

Of evaluation (pp. 72-72). Thousand Oaks, CA: SAGE Publications, Inc. doi:10.4135/9781412950558.n92

Moustakas, C. (1994). *Phenomenological Research Methods* (3rd ed.). Thousand Oaks, CA: SAGE Publications, Inc. [Kindle Cloud Reader version]. Retrieved from Amazon.com

Muegge, S., & Craigen, D. (2015). A design science approach to constructing critical infrastructure and communicating cybersecurity risks. *Technology Innovation Management Review, 5*(6), 6-16. doi:10.22215/timreview/902

National Institute of Standards and Technology. (2006). Minimum security requirements for federal information and information systems (Federal Information Processing Standards Publication 200). Retrieved from: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

National Institute of Standards and Technology. (2018). National initiative for cybersecurity education (NICE) working group. Retrieved from https://www.nist.gov/itl/applied-cybersecurity/nice/about/working-group

National Research Council. (2009). *On Being a Scientist: A Guide to Responsible Conduct in Research* (3rd ed.). Washington, DC: National Academy of Science. [Kindle Cloud Reader version]. Retrieved from Amazon.com

Nugent, P., D. & Collar, E. (2015). Where is the cybersecurity hero? Practical recommendations for making cybersecurity heroism more visible in organizations. *International Journal of Computer Science and Information Security, 13*(4), 1-5. Retrieved from

https://sites.google.com/site/ijcsis/vol-13-no-4-apr-2015

Office of the Director of National Intelligence. (2017). Background to "assessing russian activities and intentions in recent US elections": The analytic process and cyber incident attribution. Retrieved from https://www.dni.gov/files/documents/ICA_2017_01.pdf

Office of Management and Budget. (2013). Revised delineations of metropolitan statistical areas, micropolitan statistical areas, and combined statistical areas, and guidance on uses of the delineations of these areas. (OMB Bulletin No. 13-01). Washington, DC: Author.

Office of Management and Budget. (2016). Managing federal information as a strategic resource (OMB Circular A-130). Washington, DC: Author.

Oficina de Gerencia y Presupuesto. (2007, September 12). Seguridad de los sistemas de información [Security of information systems] (Policy TIG -003). San Juan, PR: Author.

Oficina de Gerencia y Presupuesto. (2007, September 12). Servicios de tecnología [Technology services] (Policy TIG-004). San Juan, PR: Author.

Oficina de Gerencia y Presupuesto. (2007, September 12). Desarrollo, integración y publicación de transacciones electrónicas gubernamentales [Development, integration, and publication of governmental electronic transactions] (Policy TIG-006). San Juan, PR: Author.

Oficina de Gerencia y Presupuesto. (2007, September 12). Uso de sistemas de información, de la Internet y del correo electrónico [Use of information

systems, the Internet, and e-mail] (Policy TIG-008). San Juan, PR: Author.

Oficina de Gerencia y Presupuesto. (2007, September 12). Adquisición de equipo para sistemas computarizados de información [Acquisition of equipment for automated information systems] (Policy TIG-010). San Juan, PR: Author.

Oficina de Gerencia y Presupuesto. (2007, September 12). Mejores prácticas de infraestructura tecnológica [Technology infrastructure best practices] (Policy TIG-011). San Juan, PR: Author.

Oficina de Gerencia y Presupuesto. (2006, July 1). Marco referencial de adquisición tecnológica gubernamental [Government technology procurement reference framework] (Policy TIG-013). San Juan, PR: Author.

Oficina de Gerencia y Presupuesto. (2011, September 12). Programa de continuidad gubernamental [Continuity of government program] (Policy TIG-015). San Juan, PR: Author.

Oficina de Gerencia y Presupuesto. (2013, April 15). Interfaz de programación - API [Application programming interface - API] (Policy TIG-016). San Juan, PR: Author.

Oficina de Gerencia y Presupuesto. (2013, April 15). Tecnológica en las nubes [Cloud computing] (Policy TIG-017). San Juan, PR: Author.

Oficina de Gerencia y Presupuesto. (2013, April 15). Revisión de contratos de tecnología [Technology contract review] (Policy TIG-018). San Juan,

PR: Author.

Oficina de Gerencia y Presupuesto. (2014, March 26). Clasificación de datos y categorización de seguridad [Data classification and security categorization] (Policy TIG-019). San Juan, PR: Author.

Orden Ejectutiva Núm. OE-2000-019 [Exec. Order No. OE-2000-019], L.A.P.R. (2000).

Orden Ejectutiva Núm. OE-2009-009 [Exec. Order No. OE-2009-009], L.A.P.R. (2009).

Orden Ejectutiva Núm. OE-2015-019 [Exec. Order No. OE-2015-019], L.A.P.R. (2015).

Orrick, D. (2012). Technology. In M. E. Beare (Ed.), Encyclopedia of transnational crime & justice (pp. 396-398). Thousand Oaks, CA: SAGE Publications, Inc. doi:10.4135/9781452218588.n153

O'Sullivan, E., Rassel, G. R., & Berner, M. (2008). *Research methods for public Administrators* (5th ed.). New York, NY: Pearson, Longman.

Patton, M. Q. (2002). *Qualitative research and evaluation methods* (3rd ed.). Thousand Oaks, CA: SAGE Publications, Inc. [Kindle Cloud Reader version]. Retrieved from Amazon.com

Paulsen, C., McDuffie, E., Newhouse, W., & Toth, P. (2012). NICE: creating a cybersecurity workforce and aware public. *IEEE Security & Privacy, 10*(3), 76-79. doi:10.1109/MSP.2012.73

Picazo-Vela, S., Gutierrez-Martinez, I., & Luna-Reyes, L. F. (2012).

Understanding risks, benefits, and strategic alternatives of social media applications in the public sector. *Government Information Quarterly, 29*(4), 504-511. doi:10.1016/j.giq.2012.07.002

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management, 51*(5), 551-567. doi:10.1016/j.im.2014.03.009

Puerto Rico Oversight, Management, and Economic Stability Act, 48 U.S.C. §§ 2101 -2241 (2016).

QSR International. (n.d.). What Is NVivo? Retrieved from http://www.qsrinternational.com/what-is-nvivo

Reece, R. P. & Stahl, B. C. (2015). The professionalisation of information security: Perspectives of UK practitioners. *Computers & Security, 48*, 82 -195. doi:10.1016/j.cose.2014.10.007

Roesener, A., Bottolfson, C., & Fernandez, G. (2014). Policy for U.S. cybersecurity. *Air & Space Power Journal*, *28*(6), 38-54. Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/a617837.pdf

Ross, R., Dempsey, & K., Pillitteri, V. (2018). Assessing security requirements for controlled unclassified information. (NIST Special Publication 800-171A). Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171A.pdf

Ross, R., Viscuso, P., Guissanie, G., Dempsey, K., & Riddle, M. (2016). Protecting controlled unclassified information in nonfederal systems and organizations (NIST Special Publication 800-171 Revision 1). Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

Rowland, J., Rice, M., & Shenoi, S. (2014). The anatomy of a cyber power. *International Journal of Critical Infrastructure Protection, 7*(1), 3-11. doi:10.1016/j.ijcip.2014.01.001

Sá, F., Rocha, A., & Pérez-Cota, M. (2015). Potential dimensions for a local e-government services quality model. *Telematics and Informatics, 33*, 270 –276. doi:10.1016/j.tele.2015.08.005

Saxby, S. (2015). The 2014 CLSR-LSPI Lisbon seminar on 'the digital citizen'– Presented at the 9th International Conference on Legal, Security and Privacy Issues in IT Law (LSPI) 15–17 October 2014, Vieira De Almeida & Associados, Lisbon, Portugal. *Computer Law & Security Review, 31*(2), 163-180. doi:10.1016/j.clsr.2015.01.011

Shafritz, J. M., Ott, J. S., & Jang, Y. S. (Eds.). (2015). Classics of organization theory. (8th ed). Belmont, CA: Wadworth, Cengage Learning. [Kindle Cloud Reader version]. Retrieved from Amazon.com

Sher, M. (2004). Group and systems theory. In G. R. Goethals G. J. Sorenson & J. M. Burns (Eds.), *Encyclopedia of leadership* (Vol. 4, pp. 612-617). Thousand Oaks, CA: SAGE Publications Ltd. doi:10.4135/9781412952392.n136

Sylves, R. T. (2015). *Disaster policy and politics: Emergency management and homeland security* (2nd ed.). Thousand Oaks, CA: SAGE Publications, Inc. [Kindle Cloud Reader version]. Retrieved from Amazon.com

Taylor, R. W., Fritsch, E. J., Liederbach, J., & Holt, T. J. (2011). *Digital crime and digital terrorism* (2nd ed.). Upper Saddle River, NJ: Prentice Hall.

Tehrani, P. M., Manap, N. A., & Taji, H. (2013). Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime. *Computer Law & Security Review*, *29*(3), 207-215. doi:10.1016/j.clsr.2013.03.011

Tellado-Domenech, R., N. (2017). El “hackeo” a Hacienda retrasa la radicación de las planillas [The "hackeo" to Hacienda delays the filing of tax returns]. El Nuevo Dia. Retrieved from http://www.elnuevodia.com/negocios/economia/nota/elhackeoahacienda retrasalaradicaciondelasplanillas-2301476/

The New Oxford American Dictionary. (n.d.). Bias. New York, NY: Oxford University Press. [Kindle Cloud Reader version]. Retrieved from Amazon.com

The New Oxford American Dictionary. (n.d.). Delimitation. New York, NY Oxford University Press. [Kindle Cloud Reader version]. Retrieved from Amazon.com

U.S. Census Bureau. (2012). San Juan-Carolina, PR combined statistical area. Retrieved from https://www2.census.gov/geo/maps/econ/ec2012/csa/ EC2012_330M200U S490M.pdf

U.S. Census Bureau. (2015a). Annual estimates of the resident population for the

United States, Regions, States, and Puerto Rico: April 1, 2010 to July 1, 2014. Retrieved from https://www.census.gov/popest/data/state/totals/2014/

U.S. Census Bureau. (2015b). QuickFacts: Puerto Rico. Retrieved from http://www.census.gov/quickfacts/table/PST045214/72

U.S. Computer Emergency Readiness Team. (n.d.). National Cyber Awareness System. Retrieved from https://www.us-cert.gov/ncas

U.S. Department of Homeland Security. (2013). Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD)-21 Critical Infrastructure Security and Resilience [Fact sheet]. Retrieved from https://www.dhs.gov/sites/default/files/publications/EO-13636-PPD-21-Fact-Sheet-508.pdf

U.S. Department of Treasury. (2015). Puerto Rico's economic and fiscal crisis. Retrieved from https://www.treasury.gov/connect/blog/Documents/Puerto_Ricos_fiscal_challenges.pdf

U.S. National Archives and Records Administration. (2018). CUI registry. Retrieved from https://www.archives.gov/cui/registry/category-list

Walden University. (2018). Research ethics & compliance: Welcome from the IRB. Retrieved from http://academicguides.waldenu.edu/researchcenter/orec/welcome

Walden University. (2015). Research ethics planning worksheet. Retrieved from http://academicguides.waldenu.edu/ld.php?content_id=16791936

Appendix A: Cybersecurity Dimensions covered by TIGs

Policy	Summary	Dimension and E-Government Goals
Development and Maintenance of Government Websites (Policy TIG-002)	Make agencies responsible for developing and maintaining websites to provide a virtual alternative to access information and services. The policy requires the development of policies and procedures for the operation and maintenance of websites in compliance with the TIG-003. The policy includes audits for the evaluation of the content, design, and usability, but not for security control.	General Context: • Increase citizen participation • Improve services • Ensure socially inclusiveness
Technology Services (Policy TIG-004)	Provides guidelines for the technology services offered by the OGP, as well as to understand the conditions and responsibilities for the services. Services such as training, licensing, firewall, email, antivirus, and consulting are not directly available to municipalities.	Organizational Structure and Processes: • Reduce costs and burdens • Improve services
Development, Integration, and Publication of Governmental Electronic Transactions (Policy TIG-006)	Outlines responsibilities and requirements regarding the development, implementation, and publication of online services. The policy requires encryption for the communication and exchange confidential information. The policy indicated the use of Secure Sockets Layer protocol but does not specify which version. **Note**: Most SSL have been deprecated by the Internet Engineering Task Force RFC 6176 and 7568.	General Context: • Increase citizen participation • Improve services • Reduce costs and burdens • Ensure socially inclusiveness

Policy	Summary	Dimension and E-Government Goals
Disposition of Equipment and Licenses (Policy TIG-007)	Describes the mechanisms to ensure that agencies properly dispose of IT hardware and software. The agencies are responsible for deciding the best method (overwriting or degaussing) to remove information, but there is not mentioned of related standards or best practices. The policy permits the transfer of obsolete equipment to other agencies. The policy does mention that equipment cannot be transferred due to security reasons but does not specify the reasons. Further, there is no mentioned of audits to validate compliance with the policy. **Note**: Obsolete technology can introduce vulnerabilities, especially as they may no longer be supported by the vendors.	Organizational Structure and Processes: • Reduce costs and burdens • Protecting privacy, security, and availability
Use of Information Systems, the Internet, and E-Mail (Policy TIG-008)	Defines the acceptable use of information handled through information systems, Internet technologies, and email to protect end users and the government from cyber incidents. The policy provides guidance without referencing standards.	Information and Data: • Protecting privacy, security, and availability
Integration of Financial Systems (Policy TIG-009)	Requires government entities to implement payroll, finance, and human resources systems providing interoperability and integration with the Hacienda.	Interorganizational Collaboration and Networks: • Promote interagency collaboration • Reduce costs and burdens

Policy	Summary	Dimension and E-Government Goals
Acquisition of Equipment for Automated Information Systems (Policy TIG-010)	Specifies the minimum standards all procurement of IT equipment must follow to ensure that it supports the e-government. The policy provides broad requirements, including • Capability to integrate with the government systems • Comply with the standards and requirements for acquisition • Meet the minimum capacity requirements and quality assurance • Comply with the TIG-003 security requirements	Organizational Structure and Processes: • Promote interagency collaboration • Reduce costs and burdens • Support procurement • Protecting privacy, security, and availability
Technology Infrastructure Best Practices (Policy TIG-011)	Establishes best practices to acquire and implement IT infrastructure components, including platforms, software, networks, and data. There is no reference to industry standards other than the Institute of Electrical and Electronics Engineers. Mandate agencies to establish methodologies to ensure the integrity, reliability, deduplication, and confidentiality of the data, but those not provide guidance.	Technology: • Reduce costs and burdens • Support procurement • Protecting privacy, security, and availability
Government Technology Procurement Reference Framework (Policy TIG-013)	This policy establishes practices that every agency within the executive branch must follow to purchase technology goods and services.	Organizational Structure and Processes: • Reduce costs and burdens • Support procurement • Protecting privacy, security, and availability

Policy	Summary	Dimension and E-Government Goals
Continuity of Government Program (Policy TIG-015)	Provides guidelines to establish programs to ensure operational continuity of critical government functions. The policy requires the use of tools and plans such as risk analysis, business impact analysis, disaster recovery plan, business continuity plan, incident management, emergency management, training, and test programs, among others. The policy follows the Disaster Recovery Institute International guidelines and practices. There is no mention of funding to accomplish these tasks. Other standards such as NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems* could be more cost-effective.	Technology: • Improve services • Protecting privacy, security, and availability
Application Programming Interface - API (Policy TIG-016)	Requires database projects to have a plan to interconnect with other agencies, including a process for defining policies, analyzing jurisdictions, validating security compliance, reviewing data classification, determining third party's interactions, and creating public policy on the particular programs and integration points. Requires compliance with privacy laws at the state and federal level but does not identify the laws. It also requires compliance with other TIGs such as TIG-003, TIG-017, and TIG-019.	Interorganizational Collaboration and Networks: • Promote interagency collaboration • Improve services • Reduce costs and burdens • Protecting privacy, security, and availability

Policy	Summary	Dimension and E-Government Goals
Data Classification and Security Categorization (Policy TIG-019).	The policy is divided into two areas. The first area provides guidance for determining the sensitivity of data to establish its proper classification and categorization. The second area relates to the protective measures to safeguard sensitive data. This policy takes advantage of federal standards and guidance. • Defines accountable roles (data owner, system owner, etc.) aligned with NIST guidelines. • Requires the use of FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* as the standard to determine security categorization. • Provide detailed guidance to secure information on physical (limited and authorized access), transit (Requires FIPS 140-2, *Security Requirements for Cryptographic Modules* compatible encryption), and storage contexts. • Requires the disposition of equipment and media to be sanitized in accordance with NIST Special Publication 800-88, *Guidelines for Media Sanitization*.	Information and Data: • Protecting privacy, security, and availability

Appendix B: Interview Protocol

Date:
Place:
Interviewer:
Interviewee: *Pseudonyms. The identity of the participant will be confidential.*
Two or more years of experience related to cybersecurity at the local government level:

Questions	Notes
1. How do you perceive the cybersecurity posture of local government municipalities in Puerto Rico in comparison with state and federal agencies?	
2. What is your organization doing to safeguard their information resources from cyber threats and do you consider it to be sufficient?	
3. What factors do you consider are most influential to achieve a resilient cybersecurity posture in municipalities within Puerto Rico?	
4. Described how these factors interconnect and their sequence or priority order.	
5. What do you think are the main challenges affecting these factors?	
6. What strategies do you recommend mitigating these challenges and improve the cybersecurity posture?	
7. What is your perception of federal and state information security policy governing cybersecurity?	
8. What do you foresee for the role of interorganizational collaboration in cybersecurity?	

Questions	Notes
9. What do you consider to be key cybersecurity related processes that need to be in place to achieve a resilient cybersecurity posture?	
10. What organizational structure do you find to be more efficient for cybersecurity management and why?	
11. How engaged are the public servants in your organization with cybersecurity and what are your recommendations to improve or sustain their level of engagement?	
12. In your experience, what are the main challenges and benefits of technology solutions to support cybersecurity operations?	
13. Anything you would like to add to this interview?	